Nortel Communication Server 1000

WLAN IP Telephony Installation and Commissioning

Release: 5.5
Document Revision: 03.04

www.nortel.com

NN43001-504

Nortel Communication Server 1000
Release: 5.5
Publication: NN43001-504
Document status: Standard
Document release date: 23 September 2008

Copyright © 2004–2008 Nortel Networks
All Rights Reserved.

Sourced in Canada

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

New in this release 9
Feature description 9
Other changes 10
Revision history 10

How to get help 11
Getting help from the Nortel Web site 11
Getting help over the phone from a Nortel Solutions Center 11
Getting help from a specialist by using an Express Routing Code 12
Getting help through a Nortel distributor or reseller 12

Overview 13
Subject 13
Resources 14
Declaration of conformity 14
Shielded cable 15
Wireless telephone network description 15
Call Server 17
DHCP Server 18
DHCP options 18
TFTP Server 18
Firewall 18
WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140 18
Components 20
Language 20
Licenses 20
Wi-Fi Multimedia 20
Wired Equivalent Privacy 21
Wi-Fi Protected Access 21
Wi-Fi Protected Access2 21
Virtual Private Network 21
Push-to-talk feature 21
Text-messaging feature 21
Loud noise environments 22
WLAN IP Telephony Manager 2245 22

Copyright © 2004–2008 Nortel Networks

WLAN Application Gateway 2246 23
Access Points 23
Handset switchover 24
Loss of signal 24

Planning 25
Challenges of integrating voice applications 26
High overhead of 802.11 26
Rate scaling and variable capacity 26
Power adjustments and variable capacity 27
Quality of Service 27
DHCP server planning 28
TFTP Server planning 30
Syslog Server planning 32
Access point planning 32
Site survey 33
Effective site survey 35
Example of AP placement 37
Solving coverage issues 38
Solving overlap issues 38
Network planning 39
Network recommendation 39
Sample Access Control List 40
Network management 40
Assessment through a WLAN site survey 41
Assessment using NetIQ Vivinet Assessor 42
Monitoring and reporting with Enterprise Network Monitoring System 43
Monitoring and reporting with Communication Server 1000 Telephony Manager 45
Monitoring and reporting with NetiQ Vivinet Assessor, Vivinet AppManager, and Vivinet Diagnostics 46
Communication Server 1000 Telephony Manager 47
Zones 47
Other network design considerations 48
Access Point interference 49
SSID options and limitations 50
Layer 3 implementation 51
WLAN IP Telephony Manager 2245 planning 52
Installation requirements 52
Capacities 53
WLAN IP Telephony Manager 2245 groups 53
Gateway and timing function 57
Roaming and handover 57
Multicast 58

Copyright © 2004–2008 Nortel Networks

Placement guidelines for the WLAN IP Telephony Manager 2245 59
WLAN Application Gateway 2246 planning 66
WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 installation requirements 67
IP address planning 67
IP addressing with DHCP 68
Planning worksheets 68

System information **71**
Bandwidth management 71
Zones 71
Zones for wireless handsets 72
Call blocking 73
Codecs 73
Jitter buffer 74
RLR and SLR 74
RTCP 74
Gain adjustment 75
Programmable rings and tones 75
In/Out of Service tones 75
Virtual Office 75
Branch Office 75
Local mode display 75
Survivable Remote Gateway 76
External Applications Server 77
End-to-end QoS 77
NAT 77
NAT Traversal feature 77
Network configurations 78
WLAN IP Telephony Manager 2245 in a NAT environment 82
DHCP Server location in a NAT environment 82
TFTP Server location in a NAT environment 83
WLAN Application Gateway 2246 in a NAT environment 83
CS 1000 features 84
IP Phone 2004 features 84

Installation **87**
Required materials 87
Supplied equipment 88
Preinstallation checklist 88
WLAN IP Telephony Manager 2245 installation tasks 88
About the front panel 88
Wall-mount 89
Rack-mount 90
LAN connection 91

Copyright © 2004–2008 Nortel Networks

Power connection 91
WLAN Application Gateway 2246 installation 91

WLAN IP Telephony Manager 2245 configuration 93
Introduction 93
Functional description 94
Configuration tasks 95
Connect to the WLAN IP Telephony Manager 2245 95
Serial port connection 96
Telnet connection 96
Configure the network 97
Save the configuration 99
Configure the WLAN IP Telephony Manager 2245 100
Change the password 102

Administration and maintenance 105
Adding a WLAN IP Telephony Manager 2245 to the system 105
Checking in to the Gateway 105
Removing a WLAN IP Telephony Manager 2245 from the system 106
Wireless handset scenarios 106
View software version 106
For the WLAN IP Telephony Manager 2245 106
For the WLAN Application Gateway 2246 107
For a wireless handset 107
Software updates 107
Update software on the WLAN IP Telephony Manager 2245 107
Update software on the WLAN Application Gateway 2246 108
Update software on a wireless handset 108
Software update (version 97.071) for the WLAN Handsets 2210/2211/2212 109
Displays 109
Wireless handset download messages 110
Normal download messages 110
Download failure or recovery messages 110

Troubleshooting 113
Troubleshooting the WLAN IP Telephony Manager 2245 113
Error Status screen 114
Network Status screen 114
Software Version Numbers screen 116
Speed or duplex mismatch 116
Troubleshooting the WLAN Application Gateway 2246 116
Troubleshooting the handset 116
Context 117
Access Point problems 117

Copyright © 2004–2008 Nortel Networks

Configuration problems 118
Duplex mismatch 118
No ring 118
Far-end echo 118
Dropped calls 119
Wireless handset status messages 119
Using Call Server overlay commands 133
TPS CLI commands 136
Determining alias IP addresses 138
Troubleshooting coverage issues 139
Before calling Nortel Technical Support 139

WLAN Application Gateway 2246 141
Introduction 141
System overview 142
Front panel 143
Third-party applications 144
Nurse-call systems 145
Installation 145
Configuring the WLAN Application Gateway 2246 IP address 146
Configuration 147
Administration console navigation 147
Task summary list 148
Configuring the OAI Box 149
Configuring network parameters 149
Connecting to the Application Server 151
Continuing configuration through Telnet 153
Connecting through Telnet 153
Configuring the Telephone Line 154
Deleting a handset 155
Searching for a handset 156
Feature programming 157
Setting or changing a password 157
System status 158
Network status 159
Software versions 160
Telephone line status 160
Certification testing 161
WLAN Application Gateway 2246 certification 161
Wireless handset certification 161
Software 161
Software updates 162
TFTP software updates Systems 163
Planning Worksheet for Handsets 164

Copyright © 2004–2008 Nortel Networks

Free the serial port for administrative purposes 165

Troubleshooting WLAN IP Telephony installations 167

Site data-gathering tables 167
Product-specific configuration 169
Terminal proxy server 169
Handsets 170
WLAN IP Telephony Manager 2245 170
Quality of Service 170
WLAN specific configuration 171
Nortel switches 171
Cisco access points and switches 171
General WLAN configuration 176
DHCP server options 177
DHCP options 178
DHCP support for handsets that emulate the IP Phone 2004 180
Format of the IP Phone 2004 Terminal DHCP Class Identifier field 180
Format of the IP Phone 2004 Terminal DHCP Encapsulated Vendor Specific option 181
Format of the IP Phone 2004 Terminal DHCP Site Specific option 182
Quality of Service checklist for voice over WLAN applications 184
RF basics and AP configuration 186
Troubleshooting 189
Diagnosis flows 189
Handset error messages 191
Timing information 192
Diagnostic Tools 193
Run Site Survey for the WLAN Handset 2210/2211/2212 193
Run Site Survey for the WLAN Handset 6120/6140 195
Diagnostics Mode 197
Syslog Mode 200
Data capture 206
Questions 206
Data checklist 206
Site-data required for the capture analysis 207
Syslog capture configuration 208
Signaling Server log capture 209
General data capture 209
Capture assert error messages with the Configuration Cradle 211
Network speech levels 212
Reference documents 212

Compatible Access Points 215

Copyright © 2004–2008 Nortel Networks

New in this release

The following sections detail what is new in *WLAN IP Telephony Installation and Commissioning (NN43001-504)* for CS 1000 Release 5.5.

Feature description

The self healing software enhancement eliminates the need for manual intervention if a WLAN Telephony Manager 2245 fails. The wireless handsets are configured with the IP address of a designated WLAN Telephony Manager 2245. As the wireless handsets register, they receive a list of IP addresses of other WLAN Telephony Manager 2245 in the network and they distribute among other WLAN Telephony Manager 2245 to share the load. This WLAN Telephony Manager 2245 becomes the registration point. The list of addresses automatically updates each time the wireless handset powers on.

If the WLAN Telephony Manager 2245 fails, the wireless handset drops active calls, then re-registers with another WLAN IP Telephony Manager 2245 in their list. The wireless handsets return to active state after this registration period. This failure does not affect other wireless handsets registered on the other WLAN IP Telephony Manager 2245 units.

The recovery period for the wireless handsets on the failed WLAN IP Telephony Manager 2245 is approximately 60 seconds.

The entire network is inoperative when new software downloads to the network of WLAN IP Telephony Manager 2245 units. When the download completes, the network comes back into service automatically.

This functionality requires WLAN IP Telephony Manager 2245 minimum software release 174.034, WLAN Handset 2210/2211/2212 minimum firmware version 97.071, and WLAN Handset 6120/6140 minimum firmware of 115.015. If any component is at an earlier release then the system works in the current master or slave mode.

Copyright © 2004–2008 Nortel Networks

Other changes

Revision history

September 2008	Standard 03.04. This document is up-issued to support CS 1000 Release 5.5. This document contains an update to technical content for WLAN IP Telephony Manager 2245.
September 2008	Standard 03.03. This document is up-issued to support CS 1000 Release 5.5. This document contains an update to technical content.
February 2008	Standard 03.02. This document is up-issued to support CS 1000 Release 5.5. This document contains an update to technical content.
February 2008	Standard 02.02. This document is up-issued to support CS 1000 Release 5.0. This document contains an update to technical content.
December 2007	Standard 03.01. This document is up-issued to support CS 1000 Release 5.5.
December 2007	Standard 02.01. This document is up-issued to support CS 1000 Release 5.0. This document includes updated content based on a maintenance release for Nortel WLAN Handset 2210/2211/2212 firmware and Nortel WLAN Telephony Manager 2245.
June 2007	Standard 01.02. This document is up-issued to reflect a change in the revision history.
May 2007	Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *WLAN IP Telephony Installation and Configuration (553-3001-304)*.
August 2005	Standard 4.00. This document is up-issued to support Nortel Communication Server 1000 Release 4.5.
September 2004	Standard 3.00. This document is up-issued to support Nortel Networks Communication Server 1000 Release 4.0.
June 2004	Standard 2.00. This document is up-issued to reflect changes in technical content.
May 2004	Standard 1.00. This document is issued to support the Nortel Networks WLAN system, including the Nortel Networks WLAN IP Telephony Manager 2245, Nortel Networks WLAN Application Gateway 2246, Nortel Networks WLAN Handset 2210, and Nortel Networks WLAN Handset 2211.

Copyright © 2004–2008 Nortel Networks

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- arrange for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the telephone number for your region:

www.nortel.com/callus

Copyright © 2004–2008 Nortel Networks

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the current ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Copyright © 2004–2008 Nortel Networks

Overview

This chapter contains information about the following topics:

- "Subject" (page 13)
- "Resources" (page 14)
- "Declaration of conformity" (page 14)
- "Shielded cable" (page 15)
- "Wireless telephone network description" (page 15)
- "Call Server" (page 17)
- "DHCP Server" (page 18)
- "TFTP Server" (page 18)
- "Firewall" (page 18)
- "WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140" (page 18)
- "WLAN IP Telephony Manager 2245" (page 22)
- "WLAN Application Gateway 2246" (page 23)
- "Access Points" (page 23)
- "Handset switchover" (page 24)

Subject

This document describes the planning, installation, configuration, maintenance, and troubleshooting for the Nortel WLAN system, including the following elements:

- Nortel WLAN IP Telephony Manager 2245
- Nortel WLAN Application Gateway 2246 (optional)
- Nortel WLAN Handset 2210
- Nortel WLAN Handset 2211

Copyright © 2004–2008 Nortel Networks

- Nortel WLAN Handset 2212
- Nortel WLAN Handset 6120
- Nortel WLAN Handset 6140

Resources

This section lists information sources that relate to this document.

- *WLAN Handset 2210 User Guide (NN10300-077)*,
- *WLAN Handset 2211 User Guide (NN10300-078)*,
- *WLAN Handset 2212 User Guide (NN10300-071)*,
- *WLAN Handset 6120 User Guide (NN43150-100)*,
- *Features and Services Fundamentals (NN43001-106)*,
- *Main Office Configuration Guide for Survivable Remote Gateway 50 (NN43001-307)*,
- *Branch Office Installation and Commissioning (NN43001-314)*,
- *IP Line Fundamentals (NN43001-500)*,
- *WLAN Handsets Fundamentals (NN43001-505)*,

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Declaration of conformity

The WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 have been found to comply with the following:

- FCC Part 15 Class A - Radiate and Conducted Emissions requirements
- CISPR 22 Class A - Radiate and Conducted Emissions requirements
- ICES 003 Class A - Radiate and Conducted Emissions requirements
- EN 55022 Class A - Radiated and Conducted Emissions requirements
- EN 55024 Immunity Requirements

Copyright © 2004–2008 Nortel Networks

- EN 61000-3-2 Harmonic Current Emissions
- EN 61000-3-3 Flicker Emissions

WARNING
Changes or modifications to this equipment not approved by Nortel can cause this equipment to not comply with part 15 of the FCC rules and void the user's authority to operate this equipment.

WARNING
This equipment contains no user-serviceable parts inside. Refer servicing to qualified service personnel.

ATTENTION
FCC CFT 47 Part 15.21 statement:
"Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense."

ATTENTION
EN 55022/SICPR22 statement:
"Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures".

Shielded cable

Nortel recommends the use of shielded cable for all external signal connections in order to maintain FCC Part 15 emissions requirements.

Wireless telephone network description

The Nortel WLAN wireless telephone network consists of the following components:

- Call Server
- DHCP server
- Trivial File Transfer Protocol (TFTP) server
- Firewall

Copyright © 2004–2008 Nortel Networks

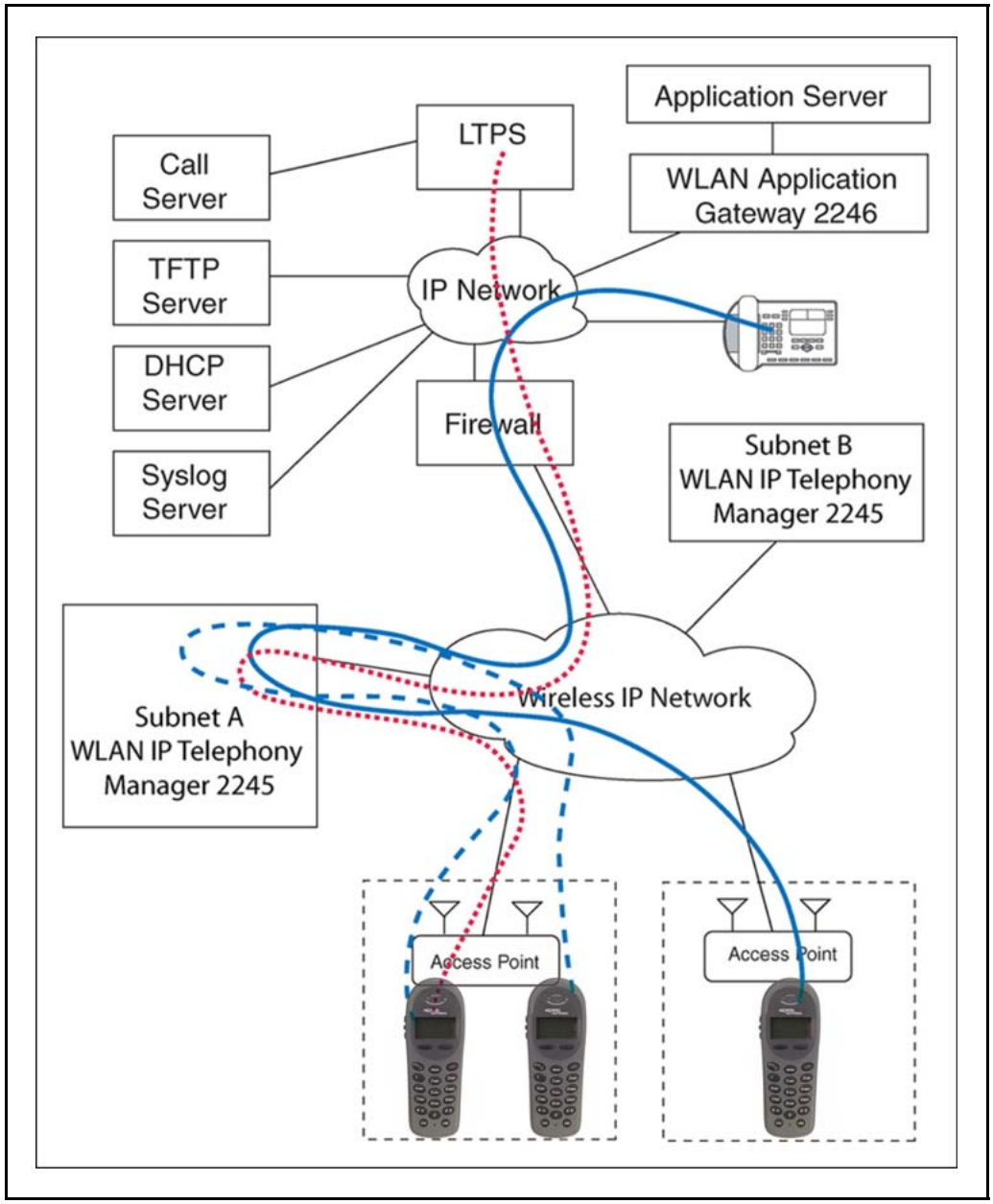
- Nortel WLAN Handset 2210/2211/2212, and Nortel WLAN Handset 6120/6140
- Nortel WLAN IP Telephony Manager 2245
- Nortel WLAN Application Gateway 2246 (optional)
- Access Point (AP)—one or more as required by the site

Figure 1 "Typical wireless telephone network configuration" (page 17) shows a typical wireless telephone network configuration. The three different lines indicate the following:

- Red—signalling
- Blue dashed—wireless to wireless audio
- Blue solid—wireless to wired audio

Copyright © 2004–2008 Nortel Networks

Figure 1
Typical wireless telephone network configuration



Call Server

The Call Server can be the Call Server of any Nortel Communication Server (CS) 1000 system running CS 1000 Release 4.5 or later software for WLAN Handset 6120/6140 and or Succession 3.0 or later for WLAN Handset 2210/2211/2212.

Copyright © 2004–2008 Nortel Networks

DHCP Server

The existing DHCP Server can be on either side of the firewall, according to the site administrator's preference. The DHCP server is optional if the wireless handsets and WLAN IP Telephony Manager 2245 are statically configured.

DHCP options

If you use a DHCP Server, configure the following options:

- DHCP Option 3—the Default Gateway
- DHCP Option 7—the Syslog Server
- DHCP Option 42—the Time Server
- DHCP Option 60—the Class Identifier
- DHCP Option 66—the IP address of the TFTP Server
- DHCP Option 151—the IP address of the WLAN IP Telephony Manager 2245
- DHCP Option 152—the IP address for the optional WLAN Application Gateway 2246

For more information, see "DHCP server options" (page 177).

TFTP Server

A TFTP Server is required in an IP Telephony system to distribute software to the wireless handsets and WLAN IP Telephony Manager 2245. It can reside on a different subnet than the Call Server and APs. The TFTP Server can be located on either side of the firewall.

Firewall

The firewall is an optional element that is often used to separate the wireless and wired domains.

WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140

The WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140 uses Voice over IP (VoIP) technology on IEEE 802.11-compliant Wireless Local Area Networks (WLANs). Access points (AP) use radio frequencies to transmit signals to and from the wireless handsets.

ATTENTION
In this document, handsets means the WLAN Handset 2210/2211/2212 and WLAN Handset 6120/6140. Where the feature refers only to a specific handset, the full handset name is used.

Copyright © 2004–2008 Nortel Networks

Employees carry wireless handsets to make and receive calls as they move throughout the building. The handsets are used only on the premises; they are not cellular phones. The handsets communicate with the CS 1000 and with the WLAN IP Telephony Manager 2245. Just like wired telephones, the wireless handsets receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long-distance calls (subject to corporate restrictions).

The handsets interoperate with other IP Line and IP Trunk features and devices, such as IP Peer, and the IP Phone 20xx and IP Softphone 2050 series of IP Phones, with the exception of some media-related constraints described in “Codecs” (page 73).

The frequencies that are allocated are governed by IEEE guidelines for WLANs and are part of the free spectrum. The WLAN Handset 6120/6140 uses a, b, and g frequencies, and the WLAN Handset 2210/2211/2212 uses the b frequency.

The handsets work only in a Nortel Succession 3.0 (and later) environment coordinated with a Communication Server (CS) 1000 or Business Communications Server (BCM). These handsets communicate with the Nortel call server through the Unified Network IP Stimulus (UNIStim) protocol. The media path of the voice call goes from the handset directly to the destination device (through the WLAN Telephony Manager 2245). In addition, the handset encapsulates all traffic in the SpectraLink Voice Priority (SVP) protocol. The WLAN Telephony Manager 2245 deencapsulates the VoIP traffic from SVP and passes it onto the network—it does not translate between UNIStim and SVP. Therefore, the Telephony Manager 2245 is in the path of all communication to and from the handset. Likewise, signaling goes from the handset to the Telephony Manager 2245 to the call server.

The WLAN Handset 2211 and the WLAN Handset 6140 are the most durable and they are the only handsets that support Push-to-talk (PTT).

For more information about the handsets, see the following publications:

- *WLAN Handset 2210 User Guide (NN10300-077)*,
- *WLAN Handset 2211 User Guide (NN10300-078)*,
- *WLAN Handset 2212 User Guide (NN10300-071)*,
- *WLAN Handset 6120 User Guide (NN43150-100)*,
- *WLAN Handsets Fundamentals (NN43001-505)*,

Copyright © 2004–2008 Nortel Networks

Components

The WLAN Handset Series 2200 offers the following components for local configuration:

- Nortel WLAN Handset 2200 Series Configuration Cradle Software—software only
- Nortel WLAN Handset 2200 Series Configuration Cradle—required hardware (serial cable included)

The WLAN Handset 6100 Series offers the following components for local configuration:

- Nortel WLAN Handset 6100 Series Administration Tool Software—software only
- Nortel WLAN Handset 6100 Series Dual Slot Handset Charger—required hardware (USB cable not included)
- USB Cable for the Nortel WLAN Handset 6100 Series Dual Slot Handset Charger

ATTENTION

For the purposes of this document

- Configuration Cradle refers to the Nortel WLAN Handset 2200 Series Configuration Cradle.
- Handset Administration Tool refers to the Nortel WLAN Handset 6100 Series Administration Tool Software.
- Dual Slot Handset Charger or Handset Charger refers to the Nortel WLAN Handset 6100 Series Dual Slot Handset Charger.

Language

The handset menus and screens that originate from the Call Server are displayed in the languages supported on the Call Server. The administration and configuration menus, and all other local handset prompts are English-only.

Licenses

The handset appears to the Call Server as a standard IP Phone 2004. Therefore, each wireless handset requires one IP User License and is subject to the same feature packaging requirements as the existing IP Phone 2004.

Wi-Fi Multimedia

The handsets support basic Wi-Fi Multimedia (WMM) to improve Quality of Service (QoS), as defined in the 802.11e specification. WMM provides prioritized QoS capability when concurrent applications, each with unique latency requirements, are competing for network resources.

Copyright © 2004–2008 Nortel Networks

When WMM is used, all voice traffic originating from the wireless handset is assigned the WMM Voice Access Category, making it the highest priority application. If the wireless network supports WMM, the handsets enable WMM support automatically; otherwise, SpectraLink Voice Prioritization (SVP) is used.

Wired Equivalent Privacy

The handsets support Wired Equivalent Privacy (WEP) as defined by the 802.11a, b, and g specification. Nortel offers the product with both 40-bit and 128-bit encryption. WEP increases the security of the wireless LAN to a level similar to a wired Ethernet LAN.

Wi-Fi Protected Access

The handsets support Wi-Fi Protected Access (WPA) using preshared key (PSK), as defined by the 802.11i specification. WPA increases the security of the wireless LAN, using key encryption, key rotation, authentication and message integrity checking.

Wi-Fi Protected Access2

The handsets support Wi-Fi Protected Access2 (WPA2) using preshared key (PSK) and Advanced Encryption Standard (AES), as defined by the 802.11i specification. WPA2 increases the security of the wireless LAN, using key encryption, key rotation, data encryption, authentication, and message integrity checking.

Virtual Private Network

The WLAN Handset 2212 supports Virtual Private Network (VPN) security. VPN security provides a secure tunnel for the transfer of unencrypted information. A two-phase approach is used to negotiate the tunnel, with Phase 1 protecting Phase 2. Phase 1 uses preshared keys, Diffie-Hellman group, hashing, and encryption. Phase 2 uses hashing and encryption. Both phases have limited, configurable lifetimes.

Push-to-talk feature

With the Push-to-talk (PTT) feature, the WLAN Handset 2211 and the WLAN Handset 6140 can operate in a PTT group-broadcast mode like a two-way radio, in addition to the standard telephone operation.

For more information, see *WLAN Handsets Fundamentals (NN43001-505)*, .

Text-messaging feature

All WLAN handsets support text messaging applications through the WLAN Application Gateway 2246. The application server communicates to the WLAN Application Gateway 2246 through a proprietary Open

Copyright © 2004–2008 Nortel Networks

Application Interface (OAI) messaging protocol. The WLAN Application Gateway 2246 forwards the messages to the WLAN IP Telephony Manager, which encapsulates the message for delivery to the handset.

If text-messaging functions are programmed, the handset can receive text messages. While you access text messages, the handset is in messaging mode. Incoming calls ring with the second call-ringing sound.

Loud noise environments

The handsets are designed to provide optimal voice quality. However, when used in extremely loud noise environments, (for example, close to working heavy machinery), degradation in call quality can be experienced due to echo. Avoid using the handsets in loud noise environments.

WLAN IP Telephony Manager 2245

The WLAN IP Telephony Manager 2245 is a device that manages IP telephony network traffic on the WLAN system. It is required to utilize the 11Mbs maximum transmission speed available in the handsets. The WLAN IP Telephony Manager 2245 acts as a proxy for the wireless handsets. It provides a number of services including a QoS mechanism, AP bandwidth management, and efficient RF link utilization.

The WLAN IP Telephony Manager 2245 works with the APs to provide Quality of Service (QoS) on the WLAN. All voice packets are encapsulated by the wireless handsets. The encapsulated voice packets to and from the wireless handsets are handled by the WLAN IP Telephony Manager 2245 and routed to and from a Call Server.

SpectraLink Voice Priority (SVP) is the QoS mechanism implemented on the wireless handsets and APs to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted and with minimum delay. SVP is fully compliant with the IEEE 802.11 and 802.11a, b, and g standards.

Nortel does not support use of ICMP Network Redirection with VoWLAN applications due to degraded routing and network performance. The Nortel 2245, upon receiving an ICMP redirect, will update its routing table and attempt to send packets through the new route, however this is not instantaneous. As per the RFC, the route is not permanent and will eventually revert to using the default gateway.

Each subnet, where the wireless handsets operate, requires at least one WLAN IP Telephony Manager 2245. One standalone unit can process up to 80 simultaneous calls depending on the model, as listed in Table 1 "WLAN Telephony Manager 2245 model numbers and capacities" (page 23). If greater capacity is required, multiple units can be used

Copyright © 2004–2008 Nortel Networks

Table 1
WLAN Telephony Manager 2245 model numbers and capacities

NTTQ60BAE5	10 simultaneous users
NTTQ60CAE5	20 simultaneous users
NTTQ60AAE5	80 simultaneous users (standard)

WLAN Application Gateway 2246

The WLAN Application Gateway 2246 is an optional device that enables third-party applications to communicate directly with up to 10 000 wireless handsets. The WLAN Application Gateway 2246 is connected to the LAN Ethernet switch through an RJ-45CAT5 cable.

For more information about the WLAN Application Gateway 2246, see “WLAN Application Gateway 2246” (page 141).

A WLAN Application Gateway 2246 supports 64 to 10 000 wireless handsets, depending on the model of Gateway, as listed in Table 2 "WLAN Application Gateway 2246 models and capacities" (page 23).

Table 2
WLAN Application Gateway 2246 models and capacities

Model number	Maximum number of users
NTTQ65AA	64
NTTQ65BA	128
NTTQ65CA	256
NTTQ65DA	512
NTTQ65EA	1024
NTTQ65FA	10 000

Access Points

802.11a, b, and g APs provide the connection between the wired Ethernet LAN and the wireless (802.11) LAN. APs must be positioned in all areas where the wireless handsets are used. The number and placement of APs affect the coverage area and capacity of the wireless system. Typically, the requirements for use of handsets are similar to that of other wireless data devices.

The APs must be either SVP-compliant or WMM-compliant to support QoS. For a list of supported APs, see “Compatible Access Points” (page 215).

Copyright © 2004–2008 Nortel Networks

Handset switchover

If a user on an active call is moving about, the call switches from AP to AP in the subnet. This changeover is transparent to the user.

Loss of signal

If a wireless handset is out of range of all APs, it waits 20 seconds for a signal to return. If a signal is not reacquired within 20 seconds, the wireless handset loses connection to the Call Server and any calls are dropped. When the wireless handset comes back into range of an AP, it reestablishes a connection to the Call Server and goes through the system registration process.

ATTENTION
If a wireless handset is out of contact with the system for four seconds (worst case scenario) during UNIStim messaging, a UNIStim failure could occur and cause the wireless handset to lose the UNIStim association with the Line Telephony Proxy Server (LTPS).

Copyright © 2004–2008 Nortel Networks

Planning

This chapter contains information about the following topics:

- “Challenges of integrating voice applications” (page 26)
- “DHCP server planning” (page 28)
- “TFTP Server planning” (page 30)
- “Syslog Server planning” (page 32)
- “Access point planning” (page 32)
- “Network planning” (page 39)
- “Network recommendation” (page 39)
- “Network management” (page 40)
- “Zones” (page 47)
- “Other network design considerations” (page 48)
- “WLAN IP Telephony Manager 2245 planning” (page 52)
- “Multicast” (page 58)
- “Placement guidelines for the WLAN IP Telephony Manager 2245” (page 59)
- “WLAN Application Gateway 2246 planning” (page 66)
- “WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 installation requirements” (page 67)
- “IP address planning” (page 67)
- “Planning worksheets” (page 68)

Copyright © 2004–2008 Nortel Networks

Challenges of integrating voice applications

The integration of voice applications on any data network causes some challenges. WLANs create a number of problems for voice, above and beyond those inherent to most data networks, such as:

- high overhead of 802.11
- rate scaling and variable capacity
- power adjustments and variable capacity
- Quality of Service (QoS)

High overhead of 802.11

Unlike many other 802.n standards, 802.11 has a very high amount of overhead associated with transmitting a packet. To compare an 802.3 network with an 802.11 network, the difference in overhead for transmitting line-rate minimum frame sizes compared to the line-rate maximum frame sizes on an 802.3 network can be significant, yet not nearly as significant as on an 802.11 network.

For 802.11, the difference in effective throughput varies dramatically with packet size because of the amount of overhead involved in transmitting a frame. Therefore, the effective throughput of the medium is potentially higher for data clients that use very large packet sizes than it is for voice clients that use smaller packets. As an example, using very conservative assumptions for average frame size, no rate scaling, and no contention or collisions, transmission overhead consumes as much as 67% of the total 802.11 medium capacity. By contrast, in an 802.3 network using the same assumptions, the overhead is about 8%.

Rate scaling and variable capacity

802.11b supports four transmission rates or data rates. Usually, as a handset gets farther from an Access Point (AP), both devices scale down to lower transmission rates to compensate for a weaker signal. As a result, a transmission at the 5.5 megabits per second (Mb/s) data rate takes approximately twice as long as the same size packet transmitted at the 11 Mb/s data rate. Longer transmission times mean less transmission time for other handsets. Therefore, rate scaling compromises the overall throughput of the medium.

Rate scaling is necessary to extend the coverage of the AP beyond a very tight region around the AP, but the effects must be taken into account when determining medium capacity. For example, if the maximum call capacity for an AP is 12 when all handsets are using the 11 Mb/s physical (PHY) layer, two handsets scaling down to 5.5 Mb/s as they move away from the AP reduces the total call capacity of that AP to roughly 10. This factor makes engineering the number of APs for the network difficult,

Copyright © 2004–2008 Nortel Networks

because handsets are roaming around and rate scaling up and down as necessary. Handsets are moving, and as they do, the engineering target of call capacity becomes a moving target.

Power adjustments and variable capacity

A WLAN has dynamic mechanisms in place for adjusting channels, adjusting power, and filling coverage holes, all in response to changes in the Radio Frequency (RF) environment. All of these mechanisms present challenges to the engineering of voice networks.

Dynamic adjustments work well for guaranteeing minimum coverage and connectivity of devices, particularly data devices. Voice requires more planned engineering.

Usually, the number of calls per area (square foot) and calls per AP determines the number of APs required to support the voice applications and devices. Power adjustments affect these parameters. If an AP increases power, it provides coverage for a larger area, meaning a greater call demand for the AP. Doubling the power of an AP can quadruple its coverage area, which means up to four times as much call demand as originally engineered. That increased coverage area also has substantial portions of lower data rate coverage. In addition, the added cochannel interference to other cells using the same channel degrades their call capacity. The net effect is that a network previously tuned for voice is now less capable of meeting the demands of voice than it was before the dynamic power adjustment.

Automatic RF changes do not always have a negative impact on voice-engineered networks. Admission control techniques help with the oversubscription problems related to increasing cell sizes dynamically. Hole filling, after an AP failure occurs, also provides substantial value to a voice solution.

When VoWLAN drives the engineering of the network both in scale and capacity, sometimes automatic RF features create more challenges than they resolve.

Quality of Service

802.11 is a shared media technology, but only one device can use the media at a time. The AP abides by this rule as well.

Because the transmitting device cannot detect collisions, 802.11 uses a statistical mechanism to reduce the possibility of collisions when two devices are ready to transmit at the same time. After the medium becomes available, the mechanism requires the devices to wait a random amount

Copyright © 2004–2008 Nortel Networks

of time before starting transmission. Because of this simple mechanism, a nonvoice device is as equally as likely to be allowed to transmit as a voice device is.

For example, if a data device does seize the medium, it can send a 1500-byte frame at the lowest data rate (if it is far away from the AP), and further delay voice frames. In addition, several data devices contending for the medium can each, in turn, send large frames before the voice device gained access to the medium.

Without a way to give preferential transmission opportunities to voice devices, supporting voice applications is a tremendous challenge on 802.11 WLANs. SpectraLink Voice Priority (SVP) has evolved into a de facto standard for Quality of Service (QoS) and serves as a model to illustrate the functions that a successful QoS mechanism can implement.

The 802.11e standard ultimately resolves QoS issues, but the delays in the standard create a number of additional implementation-specific challenges. Wi-Fi Multimedia (WMM) is a step toward full 802.11e compliance for voice and multimedia, but it is not a solution. Because it is a step, QoS feature evolution must progress towards better and more solid standards-based QoS capabilities.

WMM refines 802.11 to give statistical preference to certain classes over other classes. It is fully backward-compatible to legacy non-WMM devices, which function just like WMM best-effort class devices.

DHCP server planning

The handset IP-related parameters can be configured manually or through a DHCP server (RFC 1541 and RFC 1533). Any DHCP server can be used, but it must support the following capabilities.

- Provide Client IP address
- DHCP Option 1—Subnet Mask
- DHCP Option 3—Default Gateway
- DHCP Option 60—Class Identifier. The wireless handsets use the Class Identifier of Nortel-221x-A or Nortel-61xx-A. The DHCP server can use the string in the Class Identifier to uniquely identify a wireless handset.
- DHCP Option 66. This can be used to specify the address of the TFTP Server. If this option is not configured, the wireless handset looks at the Next server Boot server (siaddr) Option for the address of the TFTP Server* Vendor Specific Option 43, 128, 144, 157, 191, or 251. Only one of these options is required. The DHCP server encodes the

Copyright © 2004–2008 Nortel Networks

Server 1 information using the same format as the IP Phone 2004. If the Server 2 information is also present in the option, it is ignored.

- DHCP Option 151. This option contains the IP address of the WLAN IP Telephony Manager 2245. If Option 151 is not configured, the wireless handset performs a DNS lookup of the name SLNKSVP2, if Options 6 (DNS Server) and 15 (Domain Name) are configured.
- DHCP Option 152. If an optional WLAN Application Gateway 2246 is used in the system, its IP address can be specified with this option.

Each wireless handset effectively uses two IP addresses in the wireless subnet: one for the physical wireless handset and a second alias IP address that is used on the WLAN IP Telephony Manager 2245. When allocating addresses in a subnet scope on the DHCP server, a contiguous block of IP addresses as large as the number of wireless handsets supported must be marked as unavailable for distribution for other uses by the DHCP server.

When multiple WLANs are connected to a single Nortel Wireless Security Switch (WSS), the DHCP server can require specific configuration modifications. For a specific WSS that is used for special DHCP configuration requirements, see the WSS documentation.

The WLAN handsets support numerous DHCP extensions for assigning various configuration options. The WLAN handsets supply a vendor class identifier string, which in this case is Nortel-221x-A and Nortel-61xx-A. The WLAN handsets do not accept these options from the DHCP server encapsulated in a 43 Vendor Type option (which is the normal way vendor classes work). Consequently, you do not define these options as part of a vendor class on the DHCP server. Instead, you define them as new options that are assigned using the native code numbers that you give them.

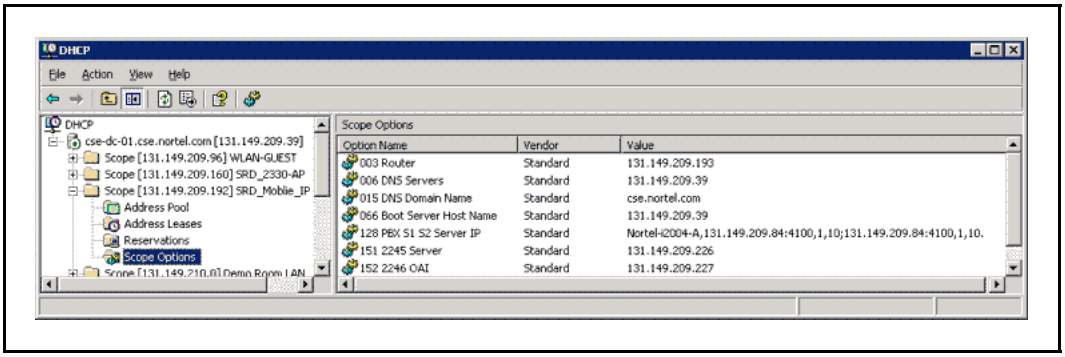
The WLAN handsets specifically request a list of options in the DISCOVER message. The list of options (aside from the IP address and subnet mask) needed by a WLAN handset is:

- Class Identifier (60)
- TFTP Server (66)
- Signaling Server Address and other parameters (43, 128, 144, 157, 191, or 251)
- WLAN IP Telephony Manager 2245 Address (151)
- WLAN Application Gateway 2246 Address (152)

For an example, see Figure 2 "Sample DHCP reservation showing assigned parameters" (page 30).

Copyright © 2004–2008 Nortel Networks

Figure 2
Sample DHCP reservation showing assigned parameters



Another use for the DHCP server is to make code upgrades to the handset easier. To prevent handsets from checking for code upgrades, assign the value of 255.255.255.255 for the TFTP server address.

A problem can arise for handset users who travel. For example, the company employing the handset solution is a retailer with many stores. Each store has a local call server for the local employees who use various VoIP devices, so all the attributes are defined at the scope level. What happens if supervisors, who travel from store to store, want to use their handsets at each location? The supervisors can be assigned to a signaling server that does not recognize their phones. The best way to support these users is to create unique reservations in each remote scope for each user's WLAN handset and specify the proper signaling server. This solution can be cumbersome if there are a large number of users who travel.

TFTP Server planning

A TFTP Server (RFC1350) holds the software images for updating the handsets and the WLAN IP Telephony Manager 2245. After the IP address of the TFTP server is configured on a wireless handset, each time the wireless handset is powered on, the wireless handset checks its version of firmware against the firmware on the TFTP Server, and if the version is different, the wireless handset downloads the new firmware from the TFTP Server. Similarly, when a WLAN IP Telephony Manager 2245 reboots, or is manually reset by the operator, it checks its version of software against the version on the TFTP Server. If the versions are different, the WLAN IP Telephony Manager 2245 downloads the new software.

The WLAN Handsets 2210/2211/2212 and WLAN Handsets 6120/6140 share the same configuration file that provides firmware version information for the TFTP process. The actual software files are specific to either the WLAN Handset 2200 series or the WLAN Handset 6100 series.

Copyright © 2004–2008 Nortel Networks

At an installation, which uses both the WLAN Handsets 2210/2211/2212 and the WLAN Handsets 6120/6140, the software files for both handset series must be installed and available on the TFTP server for the site.

Only one TFTP server is needed in the network, and it need not be colocated with the handsets or the WLAN IP Telephony Manager 2245.

There is a client-dependent aspect to how the handsets function with the TFTP server. How well a server works with the handsets can vary between code versions on the handset.

You can configure handsets to not contact the TFTP server upon boot up, by configuring 255.255.255.255 as the IP address for the TFTP server (either directly in the handset or through the DHCP option). You can configure the WLAN IP Telephony Manager 2245 to not contact the TFTP server by changing the TFTP server address to none in the configuration.

The following information must be considered when planning for a TFTP Server:

- The process for the wireless handset to check its version of firmware against what is available on the TFTP Server takes less than two seconds on a quiet network.
- If the TFTP Server is offline or unreachable, the wireless handset tries for about 10 seconds before giving up and using its existing version of firmware.
- The wireless handset firmware downloading process takes about 30 seconds.
- The TFTP Server must be capable of supporting multiple TFTP sessions.
- When a wireless handset makes a TFTP request, it uses file names without a full path name. Therefore, software updates for the WLAN IP Telephony Manager 2245 and handsets must be installed into the root directory of the TFTP Server.

When the software files are uploaded to the TFTP server. they must be unzipped. Allow time for the TFTP server to refresh and be aware of the files before attempting to download software to the wireless handsets and WLAN IP Telephony Manager 2245. Monitor the TFTP Server for any errors.

Copyright © 2004–2008 Nortel Networks

The TFTP Server can be located anywhere on the network if the wireless handsets have the subnet mask and default IP gateway configured correctly. However, the wireless handset expects a response within two seconds to any TFTP request. Therefore, the TFTP Server must not be located, for example, at the other end of a slow WAN link.

If too many wireless handsets are attempting to download new software simultaneously, the downloads can slow down or return error messages. To reduce the number of retries and error messages, manage the download process by staggering the times the wireless handsets download the software.

Nortel has tested the following TFTP servers. They are listed in order of preference.

- Nortel TFTP server (ONMS application)
- 3COM TFTP
- PumpkinTFTP

Syslog Server planning

A Syslog Server listens for incoming syslog messages on UDP port 514 and then processes the messages according to local administrative procedures. Usually the syslog messages are logged for subsequent review by the system operator. A number of devices used within a handset wireless configuration are capable of sending messages to a Syslog Server.

The Syslog Server can be any RFC 3164-compliant log server. You can configure the WLAN IP Telephony Manager 2245, WLAN Application Gateway 2246, WLAN APs 2220/2221/2230/2231, and the WLAN Handsets 2210/2211/2212/6120/6140 to generate syslog messages. For information about configuring syslog messages, see the documentation for the Wireless Security Switches and WLAN APs. For information about configuring syslog messages on the WLAN IP Telephony Manager 2245, see “Configure the network” (page 97).

There are numerous third-party Syslog Servers available. You can use any RFC 3164-compliant Syslog Server.

Access point planning

APs utilize radio frequencies to transmit signals to and from the wireless handsets.

Copyright © 2004–2008 Nortel Networks

It is essential to know where to install the APs to provide effective coverage for wireless handset use. It is necessary to verify that coverage is available where it is needed. The first step is to define exactly where the coverage is needed, which requires a site survey.

Recommendation

A site survey must be performed before installing a wireless LAN. A site survey is also recommended when an existing network structure is modified or when physical changes are made to a site.

Nortel recommends the use of the Nortel Site Survey Tool to perform the site survey.

A site survey is critical to designing and implementing a wireless LAN. The site survey is used to determine the number of APs needed to support the wireless handset users and to determine the best placement of the APs. Different AP vendors provide different tools to do this.

Site survey

To conduct a site survey, set up an AP at a particular location. Use a computer equipped with a wireless LAN device and site survey software or a handset operating in Site Survey mode to measure the strength of the signal from the AP. Move the wireless device around and repeat the measurements to determine the optimum number and best locations for the APs. This method helps identify dead zones and areas where building materials or other factors affect the performance of the network.

Site Survey mode

The handset Site Survey mode displays *negative* dBm levels. These levels represent the strength of the received signal (Received Signal Strength Indication or RSSI) from an AP. The RSSI information aids in determining if WLAN coverage is adequate.

For information about using the Site Survey mode, see *WLAN Handsets Fundamentals (NN43001-505)*, .

ATTENTION

The handsets do not require connectivity to a WLAN IP Telephony Manager 2245 or the Call Server to enable the Site Survey mode to be used. The minimum configuration required is the Extended Service Set Identifier (ESSID) of the WLAN or test AP and the WEP keys, if applicable.

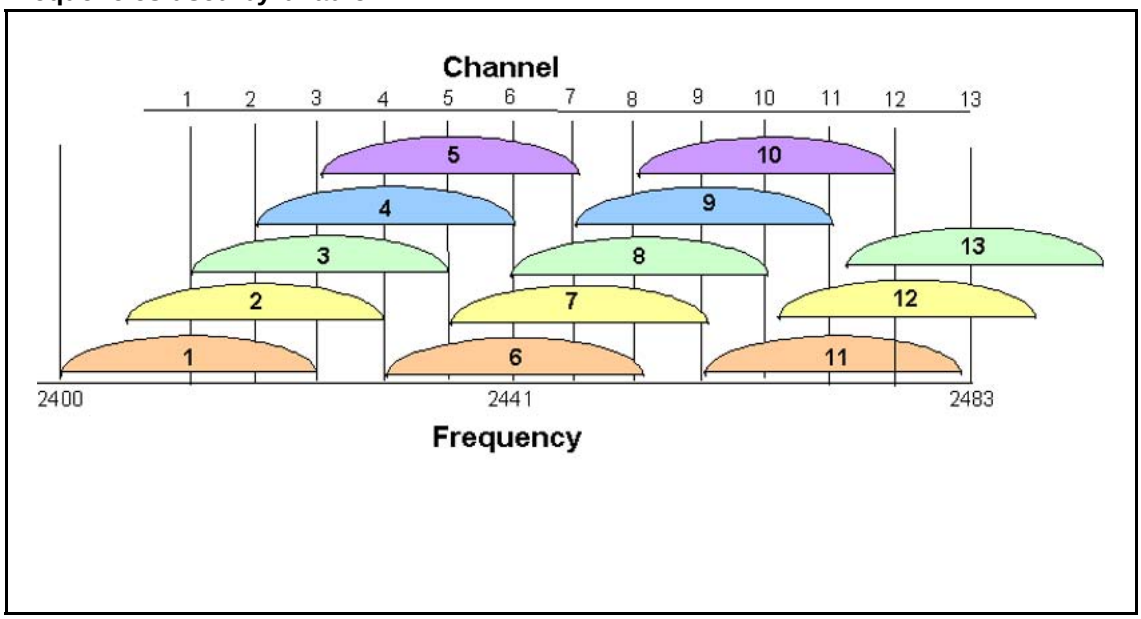
Copyright © 2004–2008 Nortel Networks

Access point requirement considerations for b radio

Each site is unique in its AP requirements. Consider the following points when determining how many APs are needed and where to place them:

- Minimum Radio Signal Strength—All APs in the coverage area must receive a signal strength better than -70dBm. Measurement is made in negative dBm, which measure the amount of signal loss due to distance. Therefore, stronger signals are those with smaller values. For example, -50 and -60 indicate stronger signals than -70; -80 is a weaker, poorer signal than -70.
- Adjacent APs and channel interference—In order to avoid undesirable interference from adjacent APs, ensure that adjacent APs do not use channels that overlap on the same frequencies.
  For more information, see Figure 3 "Frequencies used by b radio" (page 34). In the figure, channels on the same horizontal line do not overlap. In the coverage area of any given AP, signals from other APs using overlapping channels must be at least -15 to -20dBm weaker. Because the Site Survey mode displays signals only from APs on the same Extended Service Set ID (ESSID), check for signals from APs using all ESSIDs to avoid channel overlap.

Figure 3
Frequencies used by b radio



- Wireless handset range—Wireless LAN coverage must be available wherever wireless handsets are used. Although the typical range for a wireless handset is comparable to that of a laptop computer utilizing a wireless LAN PC Card, the range can not be exactly the same. Therefore, it is preferable to use a handset to carry out the site survey, if possible. Remember that wireless handsets might be used in areas where data devices are not typically used, such as stairwells, washrooms, hallways, and outdoor areas.

Copyright © 2004–2008 Nortel Networks

- Number of wireless handsets per AP—Estimate the number of wireless handsets and the anticipated call volume per AP area to ensure that the maximum number of calls per AP is not exceeded. For the maximum number of calls per AP for each supported manufacturer, see “Compatible Access Points” (page 215).
- The data rates at which the wireless handsets operate—Higher data rates (such as 11Mbs) can only be sustained while well within the range of the AP. If the wireless handsets are operating near the limits of the radio frequency (RF) coverage from the AP, they automatically drop to 1 Mbs operation.
  handsets require approximately:
  - 7% of available bandwidth per call at 11 Mbs operation
  - 10% of the available bandwidth per call for 2 Mbs operation
  - 15% of the available bandwidth per call for 1 Mbs operation.

  ATTENTION
  These requirements mean that areas with a high-use density must receive RF coverage at the highest data rate of operation.

- LAN bandwidth—Estimate anticipated peak call volume to ensure that enough bandwidth is available to handle the network traffic generated by all the wireless handsets. Handsets require approximately 150 kbps of bandwidth per call. Network traffic can be monitored and analyzed using a network sniffer or an SNMP workstation.
- Number of other wireless devices per AP—The wireless handsets can share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP.

ATTENTION
In a very large or complex site, it can be advisable to contract a professional site survey.

Effective site survey

Consider the following points for an effective site survey.

Network usage

Examine the network usage:

- How many people use a wireless handset?
- What areas of the site require wireless handset access?
- How many hours each day are wireless handsets typically in use?

Copyright © 2004–2008 Nortel Networks

- Which locations are likely to generate the largest amount of traffic?
- Where is future network expansion most likely?

Mobility requirements

Assess the mobility requirements:

- How many wireless handset users are in motion continually, such as in a warehouse or hospital?
- How many users work from different fixed locations throughout the site?

Physical site study

Perform a study of the physical site:

- Study blueprints of the proposed site. A site blueprint provides a map of the site, including the location of objects such as walls, partitions, and anything else that could affect the performance of a wireless handset. This helps identify areas where wireless handsets are less likely to perform well. Many obstructions are not readily visible and, in some cases, a room originally built for a specific purpose, such as a radiology lab, can be converted into something completely different, such as a conference room. The blueprint can also show areas proposed for future building expansion.
- Mark possible wireless handset usage locations on the blueprint and refer to the marked blueprint during the physical walk-through and inventory.

Walk-through and survey

Conduct a physical walk-through and survey:

- Document any items or materials near a proposed AP location that might interfere with reception or transmission and affect wireless handset performance, such as metal shelving.
- Document stock and inventory levels, current environmental conditions, and any materials that can interfere with wireless handset transmissions.
- Walk around the site with a site survey tool before installing APs. Use two portable computers with wireless hardware operating on a point-to-point basis. Using diagnostic software provided by the AP vendor, a coverage area for a potential AP can be determined by keeping one portable computer in one place and moving around with the other computer. Check with the vendor as to what tools are provided and what approach is recommended for deploying their APs.

Copyright © 2004–2008 Nortel Networks

RF transmission testing

After the APs are installed and configured, measure the strength of the Radio Frequency (RF) transmissions. Signal strength testing ensures that all usage areas have adequate coverage. This can be performed in two ways.

1. Use the handsets to determine AP signal strength using the Site Survey mode.
2. Use two portable computers with wireless hardware operating on a point-to-point basis. Using diagnostic software provided by the AP vendor, a coverage area for a potential AP can be determined by keeping one portable computer in one place and moving around with the other computer. Check with the vendor as to which tools are provided and which approach is recommended for deploying their APs.

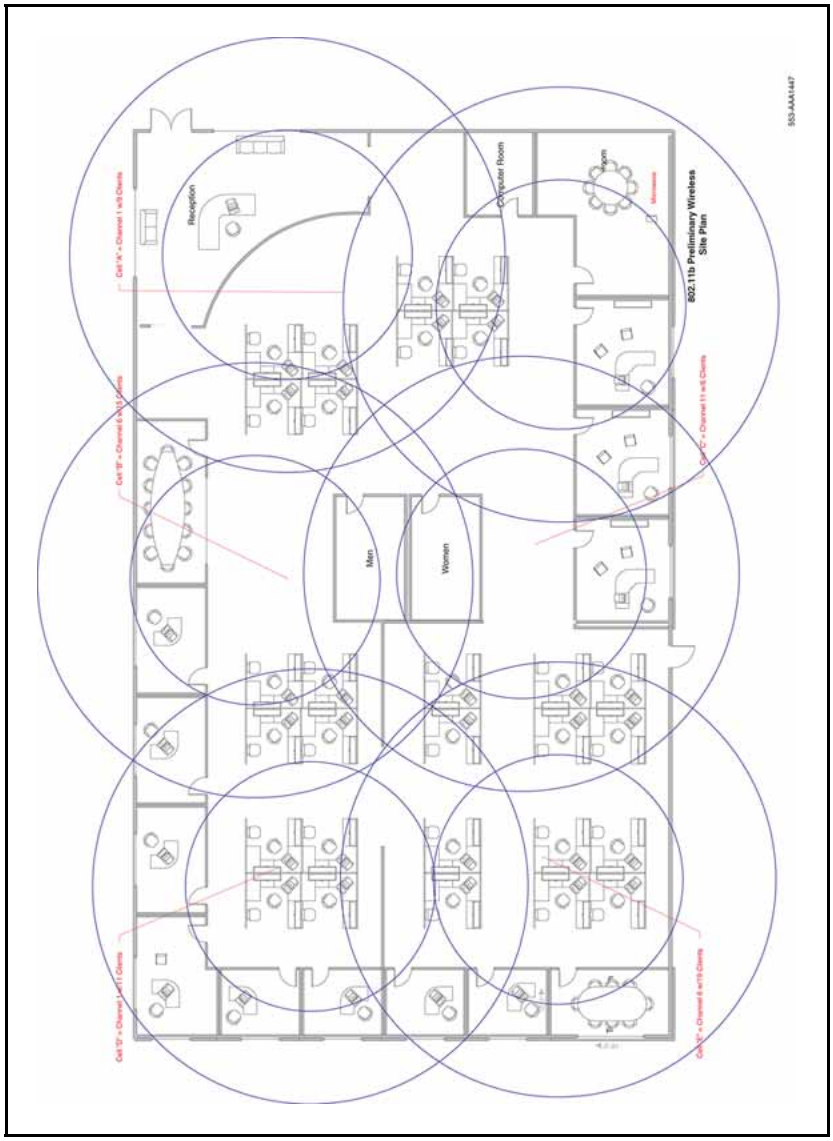
Adjust the APs as needed.

Example of AP placement

Figure 4 "Sample AP placement diagram for b radio" (page 38) is an example of an AP placement diagram based on the results of a site survey.

Copyright © 2004–2008 Nortel Networks

Figure 4
Sample AP placement diagram for b radio



Solving coverage issues

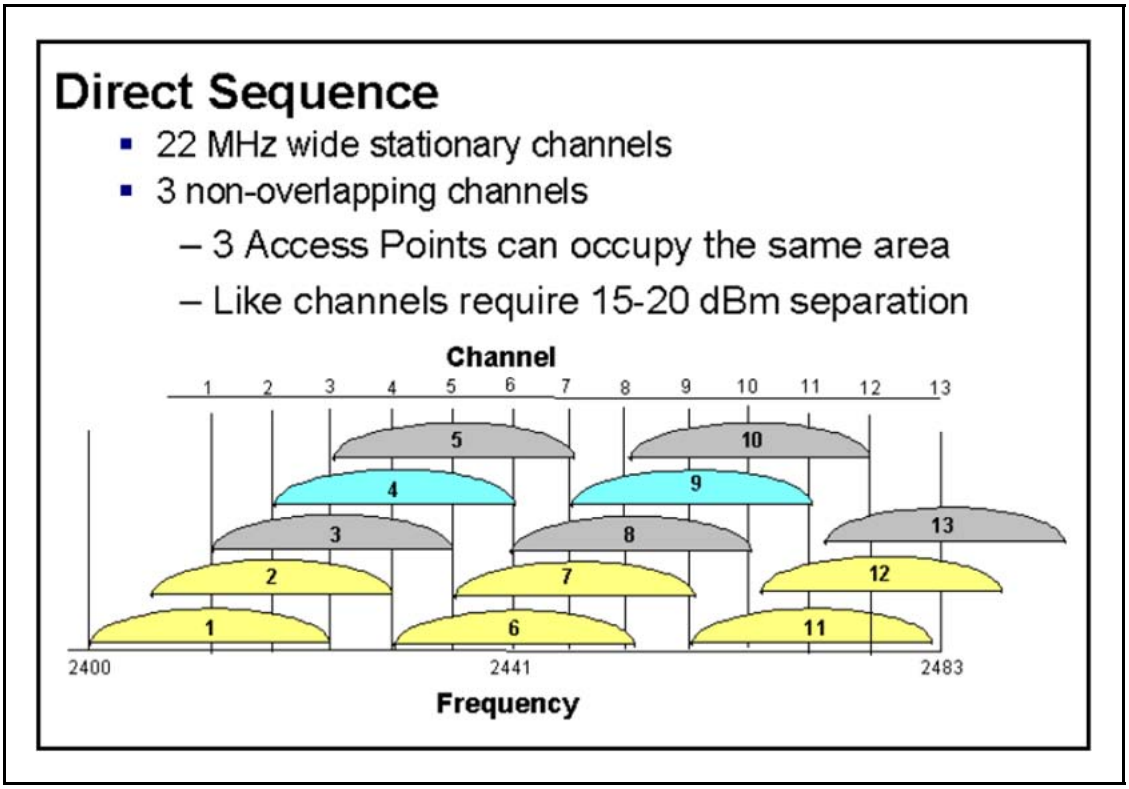
To resolve coverage issues, add and relocate APs.

Solving overlap issues

To resolve overlap issues, reassign channels to the APs or relocate the APs. Like channels require 15–20dBm separation. See Figure 5 "b radio assignment" (page 39).

Copyright © 2004–2008 Nortel Networks

Figure 5
b radio assignment



For more information about overlap, see the AP vendor documentation.

Network planning

You must ensure that all connections and interfaces for the IP Telephony network are configured as full-duplex. Duplex mismatches anywhere on the WLAN can cause the wireless IP Telephony system not to function normally.

Network recommendation

To maximize security and to minimize accessibility for unnecessary traffic to reach the WLAN Handsets, Nortel recommends that you adopt the following measures:

- Create a separate VLAN for voice traffic and map the handsets to this VLAN to mask the handsets from other devices on the network.
- Implement Access Control Lists (ACLs) on the WLAN infrastructure to contain the handsets but deny other traffic.

  — The WLAN IP Telephony 2245 uses IP protocol 119 and encapsulates both signalling and media (RTP) into a common

Copyright © 2004–2008 Nortel Networks

packet format allowing the access points to prioritize legitimate handset traffic.

— Necessary traffic for instance DHCP must be allowed, while all other traffic is denied.

Sample Access Control List

The following is a sample ACL for a voice VLAN named VLAN120.

```
set security acl ip SpectraLink permit udp 0.0.0.0 255.255.255.255
eq 68 0.0.0.0 255.255.255.255 eq 67
set security acl ip SpectraLink permit udp 0.0.0.0 255.255.255.255
eq 67 0.0.0.0 255.255.255.255 eq 68
set security acl ip SpectraLink permit cos 6 udp 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255 eq 69
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SpectraLink deny 0.0.0.0 255.255.255.255
commit security acl SpectraLink
set security acl map SpectraLink vlan VLAN120 in
set security acl map SpectraLink vlan VLAN120 out
```

Network management

Network management is as much strategy and process as it is applications. Managing a converged network consists of four key phases:

1. Assessment—Network Health Checks and WLAN Site Surveys (post-deployment) are critical assessment items. The main goal is to verify the ability of the network to provide voice at the required Quality of Experience (QoE).
2. Predeployment—Before you deploy VoIP handsets, make the network ready by rolling-out QoS across the network. This phase assumes the WLAN itself is already deployed.
3. Ongoing monitoring—Regularly monitor the performance of the converged network to ensure that voice quality continues to meet expectations as the network grows and evolves over time.
4. Reporting and planning—Keep track of exceptions and problems and form plans to resolve issues. The resolution of problems takes you back through the assessment, predeployment (QoS configuration), and monitoring phases again.

Nortel ties this business cycle together seamlessly with a set of products that provide a comprehensive solution. This solution is comprised of integrated and innovative standards-based technologies, such as Real Time Control Protocol Extended Reports (RTCP-XR) for detailed real-time management of calls in progress. The overall solution is referred to as Proactive Voice Quality Management (PVQM).

Copyright © 2004–2008 Nortel Networks

Assessment through a WLAN site survey

Technical support for VoWLAN is contingent on customers performing a site survey of the WLAN. Currently, Nortel recommends the use of the Ekahau Site Survey tool to verify the network deployment, although other site survey tools are acceptable. The Ekahau product runs on a PC and uses a WLAN network interface card (NIC) to collect data for analysis. The output of the tool is a number of robust visualizations of the network. The software verifies the basic coverage of the network and provides a number of visualizations that are useful for VoWLAN deployments.

Perform capacity planning using the data rate analysis view, which shows a color-coded view of the maximum data rate across all APs in the network. With this view, you can see where your handsets can use the 11 Mb/s data rate as opposed to scaling down to lower rates. Planning based on data rate can have a big impact on voice-call-capacity planning.

Predict AP selection and roaming using the strongest AP view. This view shows the AP with the strongest signal for each location in the building and uses color codes for each AP. With the AP view, you can predict the APs that are likely to be the primary choice of voice devices to use given their location. You can also predict where the handoff to another AP (and which AP) can occur for a moving user.

Perform resiliency planning through the AP reachability view. This view presents a color-coded visualization of the number of reachable APs from each point in the network. Locations where the tool detects one AP, locations where the tool detects two APs, locations where the tool detects three APs, and so on, are marked in distinct colors. With this visualization, you can see where the network is vulnerable to a single point of failure. It is preferable to have at least two APs that are capable of offering coverage to every point in the building.

You can also use the AP reachability view to perform location service planning. A minimum of three APs must be reachable for triangulation to be effective. Therefore, use the AP reachability feature to verify a consistent 3+ AP coverage across the building.

Location capabilities have a number of client dependencies, so verifying triangulation coverage is more complex than it appears. There are two main location-solution types:

- those that use the client to collect information about the APs in the network (client-based location)
- those that use the APs to collect information about the client (network-based location)

Copyright © 2004–2008 Nortel Networks

Both location-solution types use a form of triangulation to compute the location of the device. Depending on the power level of the AP, it can sometimes hear devices that it cannot transmit to. These factors combined create the following two scenarios:

- It is difficult to calibrate network-based solutions by using a laptop running the site survey, because APs can sometimes hear clients that cannot hear the AP. If AP transmission power levels are not at a maximum, they can hear clients over a greater distance than their own transmissions can travel. This scenario can cause the site survey application to underestimate the number of APs that can participate in triangulation.
- Client-based solutions cannot triangulate APs that are not detectable because their power is lower. But the site survey application can accurately reflect the number of APs that can be used for triangulation.

Assessment using NetIQ Vivinet Assessor

The Network Health Check is probably the most critical step toward ensuring a smooth rollout for any VoIP deployment. This statement applies even more so to VoWLAN, because a WLAN is a more challenging QoS environment than modern wired networks.

The NetIQ Vivinet Assessor 3.0 or later is the tool of choice for network health checking. (Previously NetIQ Chariot, now an Ixia product, was recommended for network health checking.) This product uses a laptop (for WLAN testing for WLAN mobility) as a voice-traffic generation and analysis tool. You can configure several nodes in various parts of the network, to simulate calls to and from those areas. Each node simulates call volumes through traffic generation so that you can stress-test access links, backbones, and WAN links as necessary. You can also configure codecs, packetization rates, and other factors to closely mimic the future VoIP environment.

Vivinet Assessor performs a comprehensive analysis of the simulated traffic, including reports on delay, jitter, and packet loss. The R values or Mean Opinion Score (MOS) are reported for these simulated traffic loads to provide a baseline for performance expectations. These analyses are also used for capacity planning because they show the capacity at which the Quality of Experience (QoE) ratings start to fall. More importantly, the process of analyzing the network reveals many latent network problems that can otherwise remain undetected until deployment.

For example, duplex mismatches can exist in various locations of the network, and data applications, being very tolerant to packet loss, typically do not reveal the problem unless it is severe. The issue is immediately

Copyright © 2004–2008 Nortel Networks

noticeable when a voice call traverses such a link. Vivinet Assessor is extremely useful for identifying the symptoms of issues and fixing such problem areas in the network long before the customer places the first call.

Monitoring and reporting with Enterprise Network Monitoring System

Enterprise Network Monitoring System (ENMS) 10.5 is a cross-portfolio management platform for fault management, network visualization, and troubleshooting. It can receive traps and statistics from the CS 1000, as well as virtually all other Nortel products. It can:

- discover the call server equipment that it supports
- display the information for the slot or port to which the call server components are attached
- discover the TLAN and ELAN connections on a CS 1000 Signaling Server

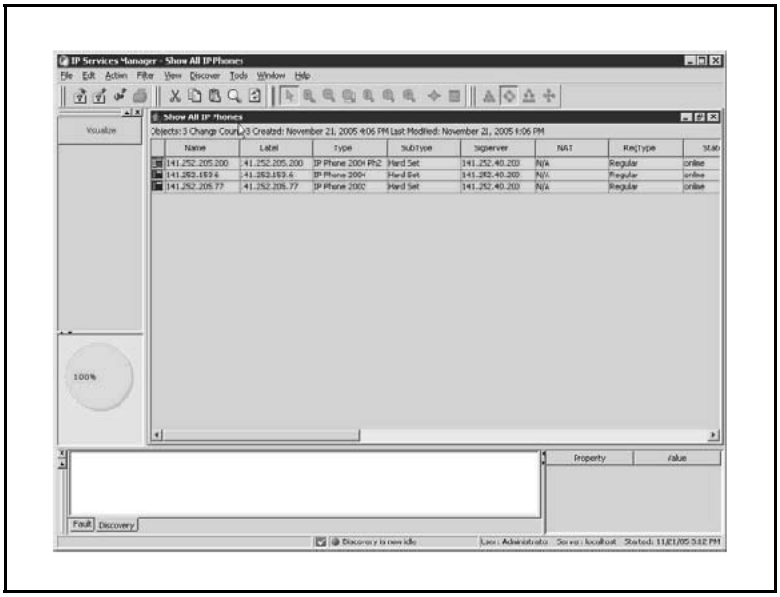
ENMS differs from the Communication Server 1000 Telephony Manager in that ENMS is a comprehensive monitoring platform for virtually all Nortel products, while Communication Server 1000 Telephony Manager supports only VoIP products and features. ENMS is the product that ties all the other management packages together.

ENMS 10.5 makes convergence management quick and easy with the Converged View in the new IP Service Management (IPSM) display. The IPSM display provides a business-oriented overview of the Convergence Service. With IPSM, an operator can see the status of overall service level that is being provided, and easily zoom in with detailed troubleshooting tools if a problem is indicated. If a phone is unreachable, or if there is a degradation of quality in a call, it is indicated in the IPSM tabular view. The call quality alert shows the near-end and far-end IP address and Terminal Number (TN).

Figure 6 "ENMS 10.5 IPSM overview" (page 44) shows the IPSM overview with a list of the phones that are registered to a particular CS 1000 system. Many details, including type of phone, firmware revision, IP address, set TN, registered TN, source, and destination IP port are displayed. Phones or components of the CS 1000 system change color to indicate status. The pie chart in the lower left corner of the display updates to show overall status and quality of the phones and CS 1000 systems in the display.

Copyright © 2004–2008 Nortel Networks

Figure 6
ENMS 10.5 IPSM overview

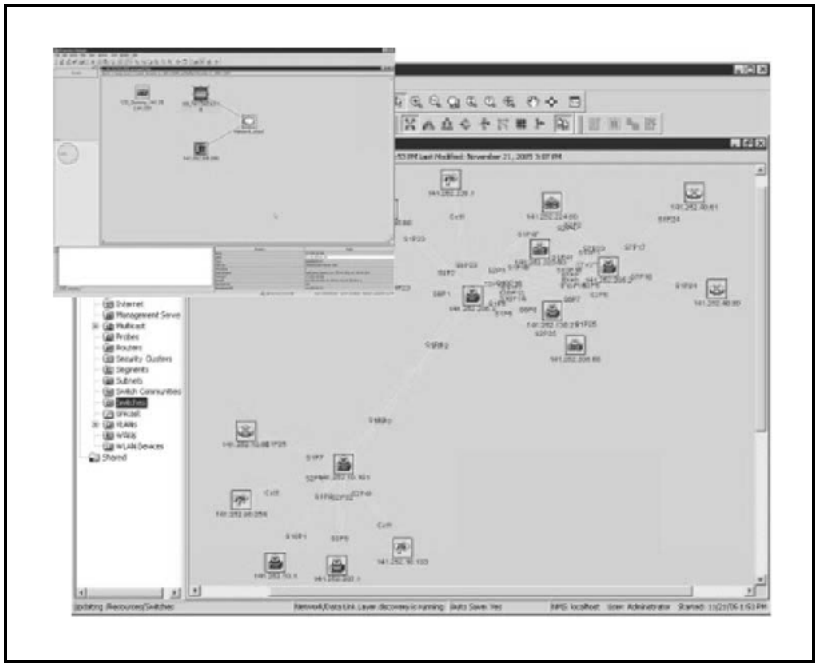


After you click on a specific IP Phone, the panel in the lower right portion of the screen displays details automatically, such as the CS 1000 system, with which the IP Phone is registered. You can then right-click on the phone to show a data network path trace graphically, as shown in Figure 7 "ENMS 10.5 IPSM convergence view" (page 45).

For troubleshooting purposes, you can view a path trace to the signaling server or any other IP address.

Copyright © 2004–2008 Nortel Networks

Figure 7
ENMS 10.5 IPSM convergence view



ENMS can provide down to physical slot port connectivity for the wired network. This topology data is extremely useful when shown in the Converged View of a Path Trace. You can set the display to refresh periodically to display the latest information about IP address changes.

With RTCP-XR, you can right-click on the set in the IPSM Convergence or tabular view and retrieve detailed real-time set statistics, such as local and remote latency and jitter.

Monitoring and reporting with Communication Server 1000 Telephony Manager

Communication Server 1000 Telephony Manager is an element manager for the CS 1000, as well as a platform for receiving traps and collecting call statistics and other performance-related data. Call and performance statistics are collected from the CS 1000 and stored on the Communication Server 1000 Telephony Manager server. You can display this data in a number of graphical reporting views, many of which are predefined for ease of use. With these features, the Communication Server 1000 Telephony Manager server can act in a basic performance-management role for voice (this is not the same thing as Proactive Voice Quality Monitoring) within the management framework.

Copyright © 2004–2008 Nortel Networks

Call tracking is another feature that is not specifically related to QoS monitoring or fault monitoring, but that is important to solution manageability. With this feature, you can:

- track calls that fit defined profiles and collect data for later trend analysis
- monitor individual extensions in real time
- have alarm notifications sent to pagers or workstations for calls that fit specified profiles

Communication Server 1000 Telephony Manager can perform some alarm-management functions and is a trap receiver for the voice products it supports. It polls call servers, through SNMP, for additional alarms that are not sent as traps. Alarms can be received from the CS 1000. Communication Server 1000 Telephony Manager can display fault information locally and also send the traps on to ENMS, Vivinet Manager, or other management platforms.

Monitoring and reporting with NetiQ Vivinet Assessor, Vivinet AppManager, and Vivinet Diagnostics

Vivinet Assessor is a Network Health Check and diagnostics tool. The software also has a number of features for the ongoing monitoring and reporting of issues. You can install Performance Endpoint agents on laptops that have WLAN interfaces, to monitor the performance and quality of the WLAN. Send this data to the Vivinet Manager for reporting and analysis. You can configure the agents with a schedule for generating VoIP traffic to run spot checks on the ability of the network to support VoIP at required quality levels.

Vivinet AppManager is a product that can be purchased separately and used in conjunction with Vivinet Diagnostics to provide detailed service-level monitoring, reporting, and troubleshooting in a diverse network environment.

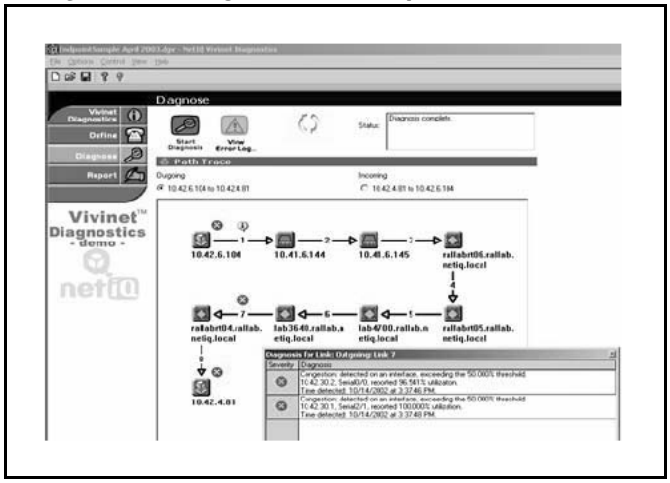
For the CS 1000, Vivnet AppManager provides information about the percentage of devices available versus unavailable, health of interfaces, Voice Call Quality and QoS for Signaling Server, and Voice Gateway Media Cards. AppManager also provides summary analysis for data loss, jitter, latency, and R-Value.

Vivinet Diagnostics is a product that can be purchased separately and used in conjunction with Vivinet AppManager. After Vivinet AppManager receives a call-quality alert from a Nortel voice system such as a CS 1000 or BCM for a call in progress, AppManager generates an alert.

Copyright © 2004–2008 Nortel Networks

The alert from Vivinet AppManager activates Vivinet Diagnostics, which traces the path of the call, collects diagnostic information, and can perform root cause analysis. You can save the results for further analysis and action. For an example, see Figure 8 "NetiQ Vivinet Diagnostics example" (page 47).

Figure 8
NetiQ Vivinet Diagnostics example



Communication Server 1000 Telephony Manager

You can configure voice devices, from stations to communication servers (including CS 1000), from the Communication Server 1000 Telephony Manager server. You can also perform station administration through the Communication Server 1000 Telephony Manager.

Although it has bulk configuration capabilities, the Communication Server 1000 Telephony Manager best serves small- to medium-size environments. For larger VoIP installations, Enterprise Subscriber Manager is a more scalable set-management platform.

Perform the actual configuration of the WLAN handsets manually or use the DHCP server. Configure the call server aspects of the handset (such as TN and DN) on the CS 1000, preferably through the Communication Server 1000 Telephony Manager.

Zones

Nortel recommends that the handsets be assigned to dedicated zones. The zones can be used to manage the bandwidth of the WLAN IP Telephony Manager 2245 groups. As well, zone designations can be used to list the wireless handsets that are currently registered or are registered using LD 117 commands.

For more information, see “Bandwidth management” (page 71).

Copyright © 2004–2008 Nortel Networks

Other network design considerations

WLAN Handsets 2210/2211/2212 are 802.11b-only devices and the WLAN Handsets 6120/6140 are 802.11b, 802.11g and 802.11a devices, which creates challenging choices for network deployments. The following list describes some of the points to consider when determining network deployment:

- Separation of devices by multiple SSIDs on the same radio does not create multiple shared mediums—the devices still transmit and receive using common radio resources on a common channel.
- Current QoS mechanisms in the industry are most effective at protecting and prioritizing traffic on the downstream, that is, from AP to Mobile Unit (MU). Wi-Fi Multimedia (WMM) improves upstream prioritization by giving a statistical edge to different classes of devices so they are more likely to transmit ahead of lower class devices. Still, other devices sometimes cheat on the contention window to gain a statistical advantage, though there are drawbacks to this method. There is no real arbitration or coordination between multiple devices that need to transmit packets upstream.
- The 802.11g devices in a mixed 802.11b/g network are statistically favored by a 2:1 ratio over 802.11b devices. For example, this means that if there is one 802.11g device and one 802.11b device and both are trying to saturate the medium with a data transfer, the 802.11g device transmits, on average, two frames for every one frame from the 802.11b device. If there are two 802.11g devices for every one 802.11b device, on average, four 802.11g transmissions occur before one 802.11b transmission occurs.
- Although 802.11g devices transmit more often, because of higher data rates, they spend less time transmitting packets. This means that 802.11g devices are not necessarily favored in the network. Having too many 802.11g devices relative to 802.11b devices upsets this balance.

There is no easy way to determine whether to maintain an 802.11g-only network or an 802.11b-only network. If there is a significant amount of upstream traffic from data devices, the best course of action is to keep data devices off the 802.11b/g network entirely. Large numbers of 802.11g devices can also cause problems with 802.11b handsets on the medium. However, if you force the 802.11g devices to use 802.11b for communication, the situation can become worse.

Disabling 802.11g support and maintaining a dual-mode 802.11a/b network can make 802.11a more attractive for dual-mode data clients and reduce the amount of data devices using the 2.4 GHz spectrum. Enabling 802.11g support can increase the number of data devices sharing the 2.4

Copyright © 2004–2008 Nortel Networks

GHz channels, which is detrimental to voice devices. As a general policy, for large amounts of data, use 802.11a for data and 802.11b for voice, but leave 802.11g disabled.

Alternately, if there are few 802.11b/g data devices and the WLAN is to be used primarily for voice, consider enabling 802.11g support. The goal is to carefully control the number of data devices that share radio resources with voice devices.

For example, if a large number of laptops exist in a campus and if 802.11g mode is enabled, it is probable that a large proportion of those laptops use 802.11g (2.4 GHz) for connectivity, which makes it much more difficult to provide good quality voice for handsets. If 802.11g is disabled, it is probable that a large proportion of those laptops use 802.11a (5 GHz) because it offers much higher throughput compared with 802.11b, and voice quality benefits.

Access Point interference

When more than three APs are deployed, the APs themselves are a significant source of interference. This is known as cochannel interference. Therefore, it is important to consider how channel reuse impacts network capacity.

To maximize the distance between APs operating on the same channel, tile the channels. To scale capacity, add more APs in the same geographic region and at the same time, reduce the transmit power of each AP.

However, the overall throughput increase does not increase proportionally with the number of APs that are added because each individual AP loses throughput, even though the number of APs per square foot is increasing. Note that the biggest loss of per-AP throughput occurs when going from nonchannel-reuse to reusing channels. For more information about this subject, see the whitepaper available from www.nortel.com.

The goal is to achieve the required call density for the number of calls per square foot. Getting the most calls per AP is not a useful objective of capacity planning. The parameters that must be tuned to engineer a voice network for capacity are:

- channel reuse factor (that is, the number of channels in the channel plan)
- transmit power of each AP
- the radius of the cell (that is, based on the physical distance between APs)

Copyright © 2004–2008 Nortel Networks

Because of the complexity of this topic and the simulation data that is required, it is not possible to discuss tuning all three variables or even two variables at a time. An example of a light to medium office environment (mostly cube space but some walls) is provided instead.

Example

The channel reuse factor for 802.11b networks is fixed at three (three nonoverlapping channels in the 2.4 GHz range), corresponding to channels 1, 6, and 11. The transmit power is fixed at 50 mW, which establishes the radius of the cell.

Now the effects of cell size, based on the other fixed parameters, can be compared.

If the deployed cells have a radius of anywhere from 33 ft to 75 ft, the call capacity per square foot is essentially the same. This means that packing cells in tighter than a 75 ft radius per AP is a waste of money. This example shows that in a typical office environment with APs at half power, you can deploy APs anywhere from 100 ft to 150 ft from each other. More walls mean there must be less distance between APs, and lowering the power of the AP lessens the required distance between APs, both of which also serve to increase the net call density.

SSID options and limitations

The traditional WLAN deployment requirement was to implement separate SSIDs for voice and for data. This requirement no longer exists, though it is still a useful deployment option in some circumstances.

If all devices implement common security encryption mechanisms (for example, Wi-Fi Protected Access), a single SSID can be offered to support both voice and data. The benefit of this configuration is that users cannot control to which network they connect. This is a security mechanism that prevents curious or malicious users from putting their laptops in the telephony VLAN. At the same time, it prevents inadvertent configuration mistakes. Either way, the simplified user interface to the network benefits both network administrators and end users.

If data devices do not use the same encryption mechanism as WLAN handsets, it is best to implement multiple SSIDs—one for the handsets and the other for the data devices.

If necessary, one way to ensure that multiple handset SSIDs on the same AP still work without oversubscribing the medium is to cut in half the number of calls per AP configured on the WLAN IP Telephony Manager 2245.

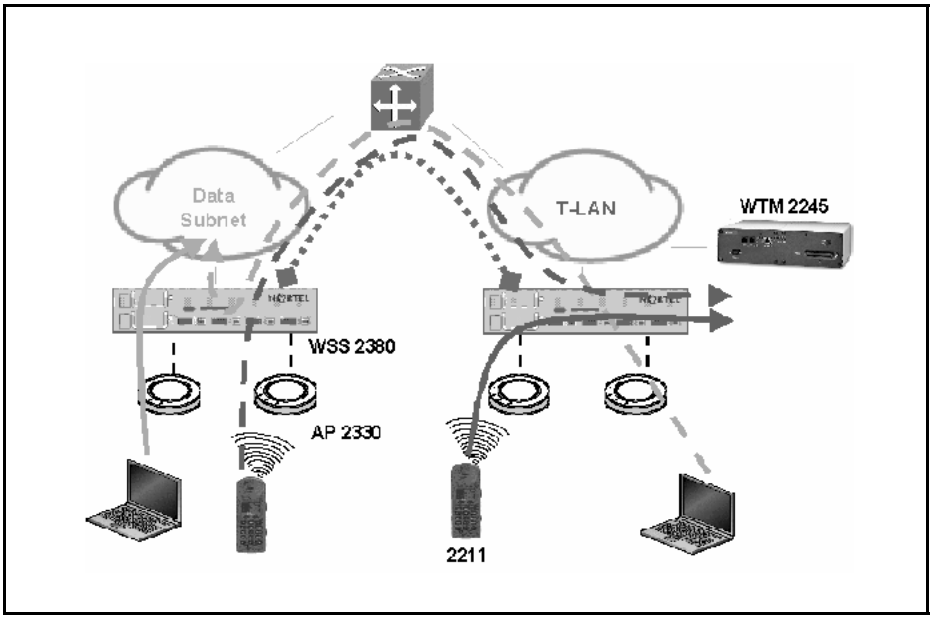
Copyright © 2004–2008 Nortel Networks

Nortel does not recommend a closed system for VoWLAN installations that use more than one SSID, including converged data and voice WLANs. The reason is that the SSID serves a valuable purpose in roaming. When it is hidden by not being included in the beacon, roaming devices must attempt to try all closed system APs. This result can dramatically impact device handoff times.

Layer 3 implementation

Where possible, simplify the number of subnets that are used for client devices. Even in a Distributed Campus architecture, you can have a few central subnets for clients. As a general rule, Nortel recommends that wired or wireless IP phones be placed in a separate VLAN (subnet) from data devices. This placement can be accomplished by providing one VLAN (subnet) for all WLAN telephony devices, as shown in Figure 9 "Single telephony VLAN implementation" (page 51). The data client VLAN design is an abstraction (the best practice is to simplify). The WLAN data network can have many client subnets, or one— that is unimportant in this context because the focus is support of VoWLAN.

Figure 9
Single telephony VLAN implementation



Consolidating VoWLAN handsets into one VLAN (subnet) has a few advantages. First, it allows the WLAN IP Telephony Manager 2245 design to be greatly simplified. Instead of purchasing and deploying at least one WLAN IP Telephony Manager 2245 per voice subnet, you can now install one WLAN IP Telephony Manager 2245 for the single voice subnet. For larger VoWLAN deployments, more WLAN IP Telephony Manager 2245

Copyright © 2004–2008 Nortel Networks

units may be required in that single subnet to support the number of calls; however, fewer WLAN IP Telephony Manager 2245 units are needed than in an equivalent multisubnet deployment.

A second advantage is that external security measures are easier and less costly to implement. It is common practice to put a telephony WLAN behind a firewall for security reasons. This is because security features on handsets, particularly authentication capabilities, tend to lag behind the industry. So to mitigate risks, you can use a firewall to block all but the ports needed for IP Telephony. This practice becomes complex and costly when multiplied by a number of subnets. A more cost-effective alternative to implementing a firewall is to assign private addresses to the handsets and let the WLAN IP Telephony Manager 2245 network address translation (NAT) capabilities serve as a form of secure firewall to the telephony LAN (T-LAN). Of course this is not as secure as using a traditional firewall to secure the T-LAN.

The downside of putting all telephony devices into the same subnet is that broadcasts are increased. Also, while security is simplified, the importance of implementing adequate security measures increases because more devices will be impacted in the event of a security breach.

Note: Nortel does not recommend running the WLAN IP Telephony Manager 2245 behind a firewall. Any routing device introduces a possibility of delay, and the higher layer routing tends to introduce longer and less predictable delays. Regularly timed packets are important in order to assure optimum voice quality, so Nortel recommends putting as little and as simple networking equipment between the WLAN IP Telephony Manager 2245 and the phones as possible.

WLAN IP Telephony Manager 2245 planning

Both the WLAN IP Telephony Manager 2245 and the WLAN Application Telephony Gateway 2246 are connected to the Ethernet switch.

Installation requirements

The WLAN IP Telephony Manager 2245 requires a CAT5 cable connection between its network port and the Ethernet switch. The WLAN IP Telephony Manager 2245 can autonegotiate to the type of port on the Ethernet switch. It supports 10BaseT, 100BaseT, full-duplex and half-duplex port types.

Nortel recommends 100BaseT full-duplex.

Copyright © 2004–2008 Nortel Networks

ATTENTION
When multiple WLAN IP Telephony Manager 2245 units are used, all the WLAN IP Telephony Manager 2245 units must use a uniform media type. Do not use full-duplex on some and half-duplex on others, or 10BaseT on some and 100BaseT on others.

Capacities

The WLAN IP Telephony Manager 2245 is available in three models:

- WLAN IP Telephony Manager 2245-80: Serves 500 powered-on handsets (80 simultaneous calls).
- WLAN IP Telephony Manager 2245-20: Serves 20 powered-on handsets.
- WLAN IP Telephony Manager 2245-10: Serves 10 powered-on handsets.

Capacity is measured by active calls for the WLAN IP Telephony Manager 2245-80 and by powered on handsets for the WLAN IP Telephony Manager 2245-10 and the WLAN IP Telephony Manager 2245-20. The capacity of a system that is not based on 100Base-T, full-duplex is lower. Nortel recommends that you not use older technology equipment.

In any subnet where wireless handsets are used, each subnet must have one or more WLAN IP Telephony Manager 2245 units. A WLAN IP Telephony Manager 2245 group on a subnet consists of one or more WLAN IP Telephony Manager 2245 units and their associated wireless handsets.

WLAN IP Telephony Manager 2245 groups

WLAN IP Telephony Manager 2245 groups are those that have more than one WLAN IP Telephony Manager 2245 in order to accommodate larger systems and a higher volume of wireless telephony traffic.

In a group comprised of multiple WLAN IP Telephony Manager 2245 units, the wireless handsets are configured with the IP address of a designated WLAN IP Telephony Manager 2245. As the wireless handsets register with the designated WLAN IP Telephony Manager 2245, they receive a list of other WLAN IP Telephony Manager 2245 units in the network. The wireless handsets distribute among the WLAN IP Telephony Manager 2245 units to share the load, which then becomes their registration point.

Copyright © 2004–2008 Nortel Networks

WLAN IP Telephony Manager 2245 failure

After the initial registration, if a WLAN IP Telephony Manager 2245 units fails, the following occurs:

1. The wireless handset drops active calls.
2. The wireless handset then re-registers with another WLAN IP Telephony Manager 2245 units.
3. The wireless handset returns to the active state.
   The recovery period is approximately 60 seconds.

The WLAN IP Telephony Manager 2245 failure has no effect on other wireless handsets registered to other WLAN IP Telephony Manager 2245 units.

Group capacities

The number of calls that an individual WLAN IP Telephony Manager 2245 can support is dependent on the number of WLAN IP Telephony Manager 2245 units in the subnet. Assuming that a 100 Mb/s full-duplex connection to the network exists, a single stand-alone WLAN IP Telephony Manager 2245 unit can manage up to 80 active calls. If two WLAN IP Telephony Manager 2245 units are installed , each can support up to 64 active calls for a total of 128 calls.

Table 3 "Multiple WLAN IP Telephony Manager 2245-80 capacities" (page 54) lists the call capacities for WLAN IP Telephony Manager 2245-80 groups. Table 4 "Multiple WLAN IP Telephony Manager 2245-10 and 2245-20 capacities" (page 55) lists the handset capacities for WLAN IP Telephony Manager 2245-10 and 2245-20 groups.

Table 3
Multiple WLAN IP Telephony Manager 2245-80 capacities

Number of WLAN IP Telephony Manager 2245 units	Calls per WLAN IP Telephony Manager 2245 units	Total calls	Erlangs	Number of wireless handsets 10% use	Number of wireless handsets 15% use	Number of wireless handsets 20% use
1	80	80	65	500	433	325
2	64	128	111	1000	740	555
3	60	180	160	1500	1067	800
4	58	232	211	2000	1407	1055
5	57	285	262	2500	1747	1310
6	56	336	312	3000	2080	1560
7	56	392	367	3500	2447	1835

Copyright © 2004–2008 Nortel Networks

Table 3
Multiple WLAN IP Telephony Manager 2245-80 capacities (cont'd.)

Number of WLAN IP Telephony Manager 2245 units	Calls per WLAN IP Telephony Manager 2245 units	Total calls	Erlangs	Number of wireless handsets 10% use	Number of wireless handsets 15% use	Number of wireless handsets 20% use
8	55	440	415	4000	2767	2075
9	55	495	469	4500	3127	2345
10	55	550	524	5000	3493	2620
11	55	605	578	5500	3853	2890
12	54	648	621	6000	4140	3105
13	54	702	674	6500	4493	3370
14	54	756	728	7000	4853	3640
15	54	810	782	7500	5213	3910
16	54	874	836	8000	5573	4180

Table 4
Multiple WLAN IP Telephony Manager 2245-10 and 2245-20 capacities

Number of WLAN IP Telephony Manager 2245 units	Number of handsets WLAN IP Telephony Manager 2245-10	Number of handsets WLAN IP Telephony Manager 2245-20
1	10	20
2	20	40
3	30	not applicable
4	40	not applicable

For example, if there are two subnets for handsets in a campus and some handsets are directed to one subnet and some to the other, there are two Call Admission Control domains operating independently. Specifically, if both specified a limit of seven calls for each AP, it is possible to have seven calls admitted by each WLAN IP Telephony Manager 2245 on the same AP—therefore, the AP is oversubscribed by 2:1.

If multiple subnets are required, the best way to support them is to leverage the Layer 3 WLAN IP Telephony Manager 2245 design. With this design, the WLAN IP Telephony Manager 2245 units are clustered in one subnet and the traffic from the handset is routed from the appropriate WLAN IP Telephony Manager 2245 unit in the cluster. Although this is a supported configuration, all the engineering guidelines for latency, jitter,

Copyright © 2004–2008 Nortel Networks

and packet loss must still be maintained. The Layer 3 design guidelines for having clients and WLAN IP Telephony Manager 2245 in different subnets does not mean that the WLAN IP Telephony Manager 2245 clustercan also be separated by routers. All the WLAN IP Telephony Manager 2245 units in the cluster must still be collocated in the same subnet.

WLAN handsets

The WLAN Handsets 2210/2211/2212/6120/6140 support both G.711 and G.729 codecs, but only using a 30 ms packetization rate.

The WLAN IP Telephony Manager 2245 translates between packetization rates, meaning that from the WLAN IP Telephony Manager 2245 to the handset, the call uses the packetization rate specified by the CS 1000 (for example, 20 ms). Nortel recommends that the CS1000 paketization rate match the 2245 at 30ms. For BCM, the packetization rate must be 30ms.

The handsets encapsulate their voice payloads in SVP for QoS. The handsets further synchronize communications, so that the handsets are able to avoid collisions with each other more effectively than the usual 802.11 collision avoidance mechanisms. Each handset maintains a list of up to four APs as potential candidates for roaming. The handsets are aggressive in roaming to other APs, which tends to prevent them from using a suboptimal data rate when another AP can provide better service. The handsets also communicate with the WLAN IP Telephony Manager 2245 and discover which APs are at full call capacity, so that the handsets can direct their calls through an AP that has call capacity available.

Under optimal conditions, meaning no interference and all devices in proximity of the AP, up to 10 voice calls from a handset are supported on a single AP 2330. When configuring the maximum call parameter of a WLAN IP Telephony Manager 2245, never configure it above 10. A more realistic rule of thumb that allows for devices to move about and rate scale accordingly is anywhere from six to eight calls per AP. A noisy RF environment can impact the numbers further.

To provide data devices some amount of guaranteed bandwidth, lower the maximum voice calls per AP to prevent voice calls from consuming all available throughput. For example, limiting the maximum calls per AP to seven allows data traffic to reserve up to 30 per cent of media capacity. If the network supports other handset calls on the 802.11b network, you must leave adequate capacity for those calls too. Note that the call admission control function of the WLAN IP Telephony Manager 2245 cannot serve to limit those other voice calls on a per-AP basis.

Copyright © 2004–2008 Nortel Networks

There is an alternative control on the WLAN IP Telephony Manager 2245 that affects call capacity across APs. This control allows the WLAN IP Telephony Manager 2245 to fix the data rates that handsets use. The options are Automatic and 1 Mb/2 Mb only. When you choose the latter, maximum call capacity drops by slightly more than half if G.711 is in use, or by slightly more than two-thirds if G.729 is in use. Most of the variability of call capacity is removed as rate scaling effects are eliminated. Therefore, you can get more predictable call capacity at the expense of maximum number of calls under optimum conditions. Note that with this option enabled, throughput for 802.11b data devices is severely impacted by even one or two voice calls.

If the automatic option to have higher potential capacity is selected, there is a risk of occasionally being oversubscribed under the worst conditions. For example, if eight calls is the configured limit on the WLAN IP Telephony Manager 2245, and if all eight calls are from handsets on the edge of coverage, the cell is oversubscribed. If five calls is the configured limit and handsets are restricted to 1 Mb/2 Mb, capacity is wasted when most handsets are close that could otherwise be used by other data devices.

To gain this type of predictability, engineer the maximum calls per AP based on 1 Mb/2 Mb rate selections in the handsets, configure that number as the call limit on the WLAN IP Telephony Manager 2245, and then configure the actual rate of the handsets (on the WLAN IP Telephony Manager 2245) to Automatic. That way, the WLAN is engineered for the worst case, but in optimal conditions, more throughput is left over for other devices to use, because the handsets use higher data rates.

To summarize, do not use the 1 Mb/2 Mb option, even if the network is engineered to that type of coverage.

Gateway and timing function

WLAN IP Telephony Manager 2245 units provide both the connection or gateway to the Call Server for the wireless handsets, and the timing function for active calls. This gateway function is distributed across the WLAN IP Telephony Manager 2245 group.

The number of active WLAN IP Telephony Manager 2245 units is determined dynamically. Whenever a WLAN IP Telephony Manager 2245 is added to or removed from the system, the distribution of timing function for active calls, as well as the gateway function, is affected.

Roaming and handover

Roaming is the ability of the wireless handset to go anywhere in the WLAN Extended Service Set RF signal coverage area, and to make and receive calls. Handover is the ability of the wireless handset to maintain an active

Copyright © 2004–2008 Nortel Networks

call without interruption while moving within a WLAN Extended Service Set (ESS) RF signal coverage area of a WLAN. This means that the wireless handset hands over the WLAN RF signal from AP to AP without interrupting the data stream.

Access points on the same subnet

The handset can perform handover and roaming across SVP-compliant APs that reside on the same subnet as the wireless handset and WLAN IP Telephony Manager 2245 group.

Mobility across different subnets when using DHCP

If a WSS is not in use and the wireless handset IP address is acquired through DHCP, the wireless handset must be powered down and powered up when entering a new subnet. This enables functionality of the wireless handset when entering the WLAN RF signal coverage area of a different WLAN IP Telephony Manager 2245 group on a different subnet. After the wireless handset establishes communication within the Extended Service Set Identifier (ESSID) of the new WLAN, obtains another IP address from the DHCP server, and normal functionality returns. If the wireless handset is configured to use ESSID of the new WLAN, it automatically discovers the ESSID of the APs operating in broadcast mode.

Table 5 "Roaming and handover capabilities summary" (page 58) summarizes the capabilities.

Table 5
Roaming and handover capabilities summary

IP address	WSS in use	Roaming capability	Handover capability
Static	No	No	No
Static	Yes	Yes	Yes
DHCP	No	Yes, if the wireless handset is power-cycled between subnets.	No
DHCP	Yes	Yes	Yes

Multicast

IP multicast addresses are used by the WLAN Handset 2211 and the WLAN IP 6120 Handset Push-to-talk (PTT) feature. The use of IP multicast addresses requires that multicasting be enabled on the Layer 2 switch used by the defined group (WLAN IP Telephony Manager 2245 units and wireless handsets).

Copyright © 2004–2008 Nortel Networks

Routers are typically configured with filters to prevent multicast traffic from flowing outside of specific domains. The wireless LAN can be placed on a separate VLAN or subnet to reduce the effects of broadcast and multicast traffic from devices in other network segments.

Placement guidelines for the WLAN IP Telephony Manager 2245

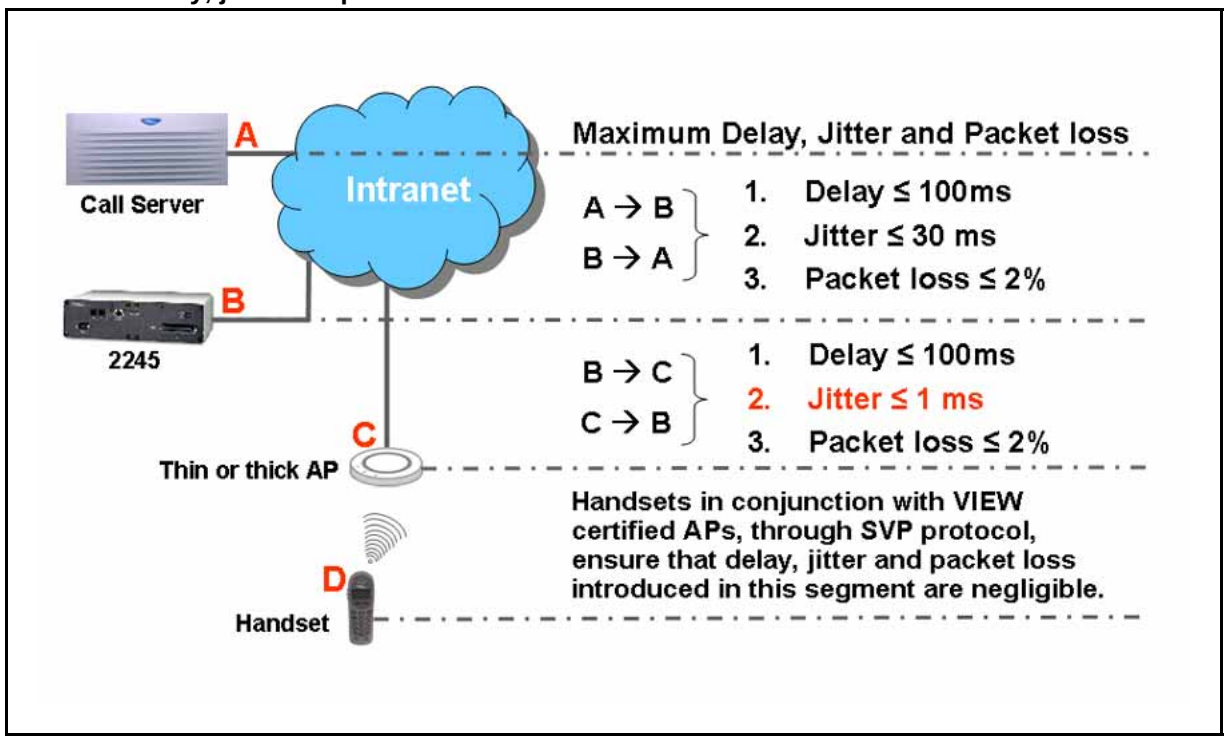
To reduce the impact that jitter, delay and packet loss has on voice quality, proper placement of the WLAN IP Telephony Manager 2245 is critical. See Figure 10 "Maximum delay, jitter and packet loss" (page 59). The WLAN IP Telephony Manager 2245 provides three critical functions to help achieve exceptional voice quality over WLAN:

- Timing
- Quality of Service (QoS)
- Connection Admission Control

Before adding the WLAN IP Telephony Manager 2245 to the network:

- Ensure that the APs used in the network are Voice Interoperability for Enterprise Wireless (VIEW) certified. For more information, go to www.spectralink.com/consumer/partners/view_certification.jsp.
- Ensure that the handsets are running Nortel Phase II software (97.070 or greater).

Figure 10
Maximum delay, jitter and packet loss



Copyright © 2004–2008 Nortel Networks

Strict timing requirements dictate that the WLAN IP Telephony Manager 2245 must be placed as close as possible to the handsets, ideally in the same subnet.

End-to-end jitter, delay and packet loss budget is a general VoIP best practice:

- End-to-end delay is the time it takes for voice to go from the microphone of the sending telephone to the earpiece of the receiving telephone.
- End-to-end jitter must not exceed 30 ms north of the SVP server (PBX to the WLAN IP Telephony Manager 2245) and must not exceed 1 ms south of the SVP server (the WLAN IP Telephony Manager 2245 to the AP).
- End-to-end packet loss is the number of packets that are lost in the network.

To achieve excellent voice quality, Nortel recommends using G711 CODEC with the following configuration:

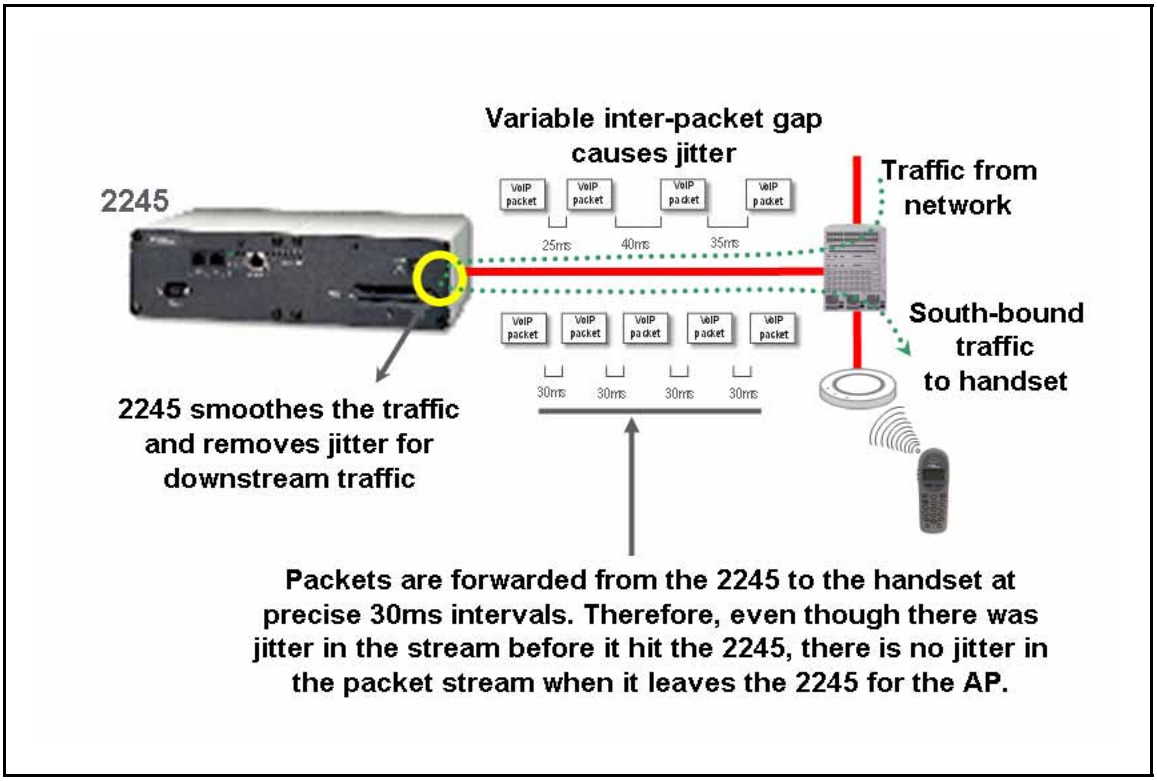
- End-to-end delay < = 150 ms (one way)
- Packet loss < = 0.5%
- The maximum jitter buffer for the handsets set as low as possible.

For more information, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*, .

The jitter budget for the link south of the WLAN IP Telephony Manager 2245 ensures that packets arrive at the handset within the 30 ms arrival window. The evenly spaced packet flow on the outbound side of the WLAN IP Telephony Manager 2245 allows the handset to conserve battery life by not using extra battery power to wait for late arriving packets. It also allows efficient roaming while the handset moves from one AP coverage area to another. See Figure 11 "Jitter removal for packets going to the AP" (page 61).

Copyright © 2004–2008 Nortel Networks

Figure 11
Jitter removal for packets going to the AP


Variable inter-packet gap causes jitter
2245
VoIP packet
25ms
40ms
35ms
Traffic from network
South-bound traffic to handset
30ms
2245 smoothes the traffic and removes jitter for downstream traffic
Packets are forwarded from the 2245 to the handset at precise 30ms intervals. Therefore, even though there was jitter in the stream before it hit the 2245, there is no jitter in the packet stream when it leaves the 2245 for the AP.

The following figures describe end-to-end delay for differing topologies:

- For an example of an end-to-end delay for a LAN, see Figure 12 "Example 1: End-to-end delay and packet loss for a LAN" (page 62).
- For an example of an end-to-end delay for a WAN, see Figure 13 "Example 2: End-to-end delay and packet loss for a WAN" (page 62).
- For an example of an end-to-end delay for a LAN to a Public Switched Telephone Network (PSTN), see Figure 14 "Example 3: End-to-end delay and packet loss for a LAN to a PSTN" (page 63).

Copyright © 2004–2008 Nortel Networks

Figure 12
Example 1: End-to-end delay and packet loss for a LAN

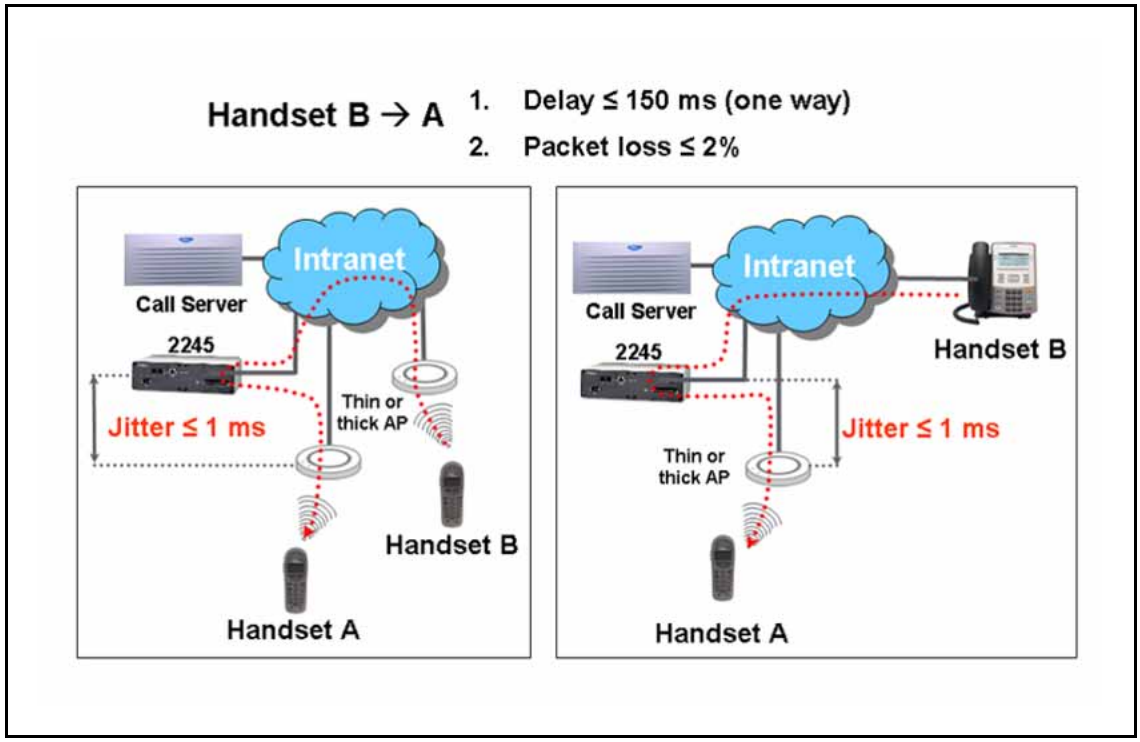
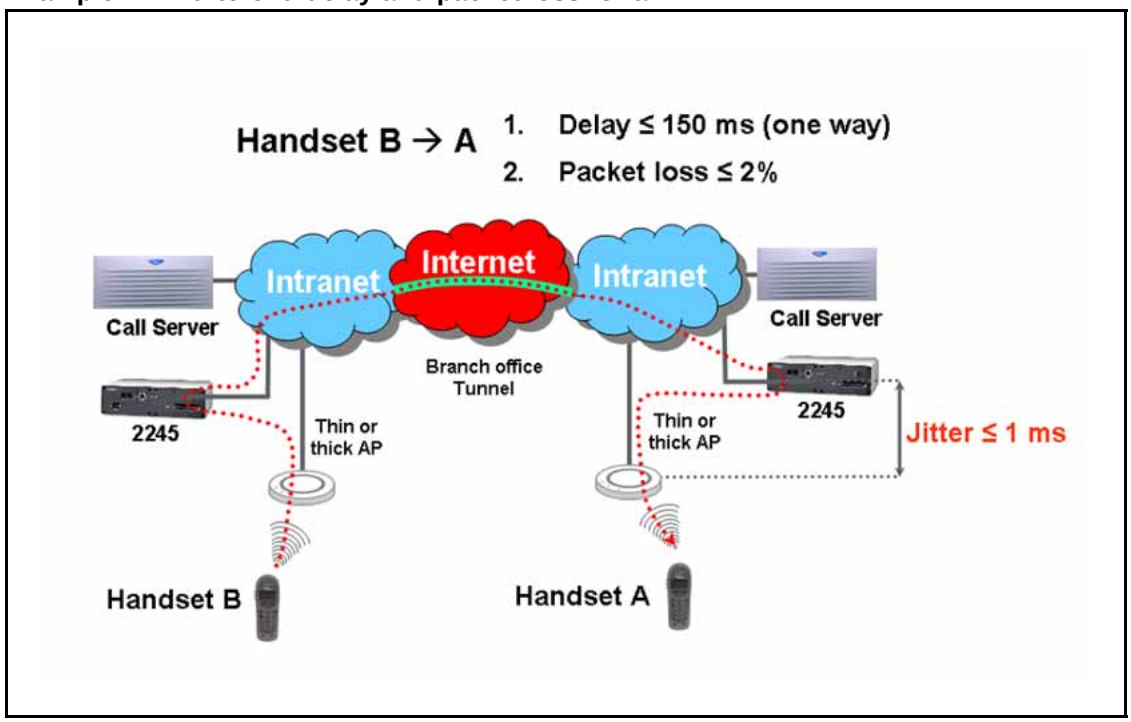
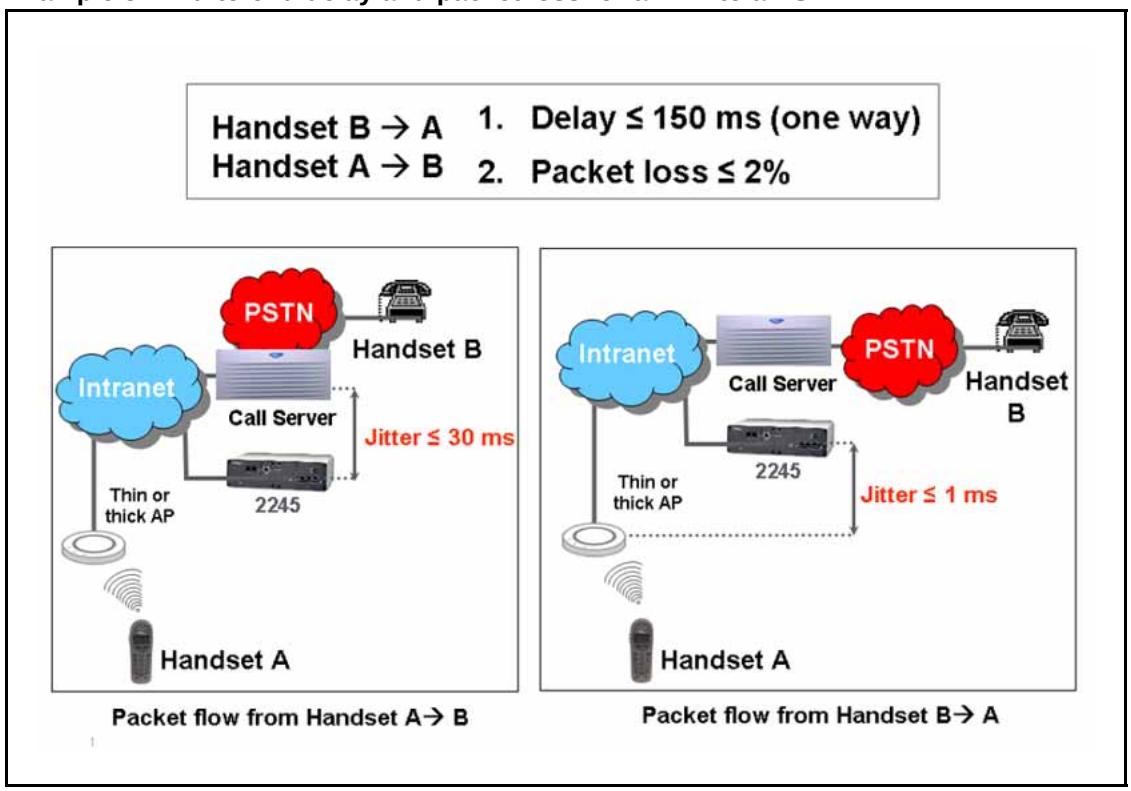


Figure 13
Example 2: End-to-end delay and packet loss for a WAN



Copyright © 2004–2008 Nortel Networks

Figure 14
Example 3: End-to-end delay and packet loss for a LAN to a PSTN



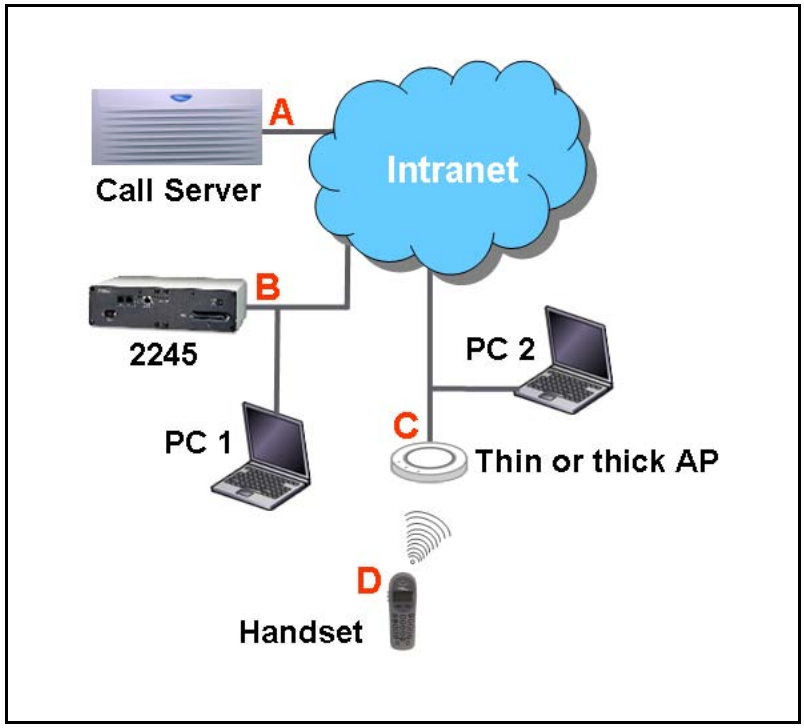
Use the following tools to measure jitter, delay and packet loss:

- Ping (to estimate delay and packet loss)
- Netmeeting (to generate RTP traffic)
- Ethernet (to capture and analyze the RTP traffic)

For more information, see Figure 15 "Measuring jitter, delay and packet loss" (page 64) and Procedure 1 “Measuring jitter, delay, and packet loss” (page 64).

Copyright © 2004–2008 Nortel Networks

Figure 15
Measuring jitter, delay and packet loss



Procedure 1
Measuring jitter, delay, and packet loss

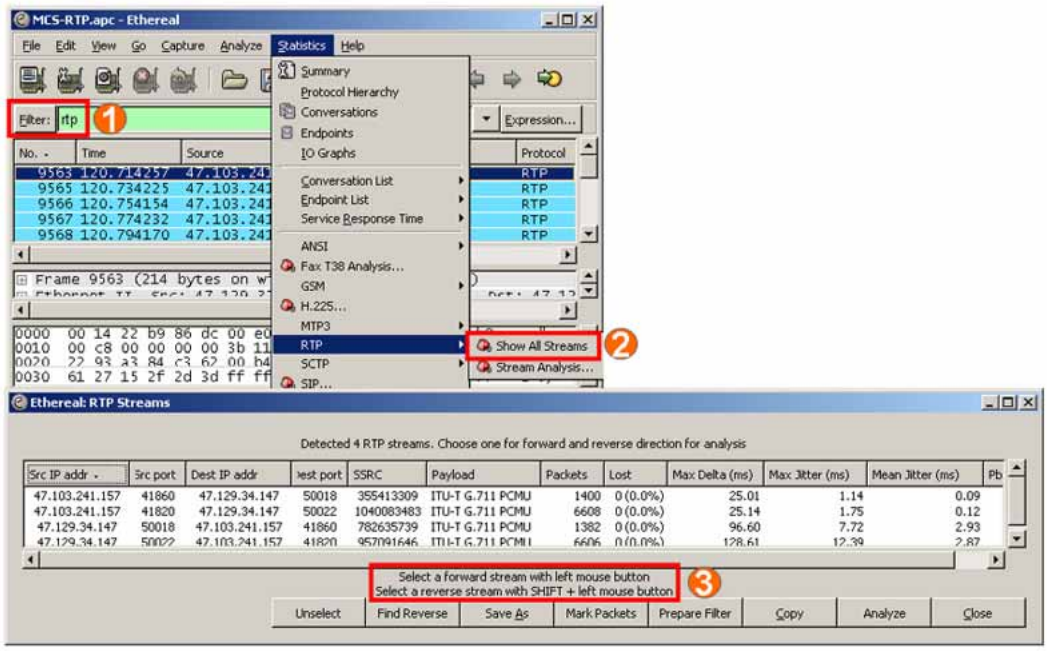
Step	Action
1	Connect PC 2 to LAN segment C.
2	Obtain the IP address of PC 2.
3	Start Netmeeting.
4	Connect PC 1 to the LAN on segment B.
5	Ping PC 2 and note the length of the round-trip delay.
6	Start Ethernet and capture packets on the correct interface.
7	Configure a filter for RTP packets.
8	Start a Netmeeting session on PC 2.
9	End the Netmeeting session and stop the packet capture.
10	Save the file and analyze the trace to make sure that the jitter, delay, and packet loss are within specifications.
11	Move PC 2 to segment A and repeat Step 1 to Step 10.

--End--

Copyright © 2004–2008 Nortel Networks

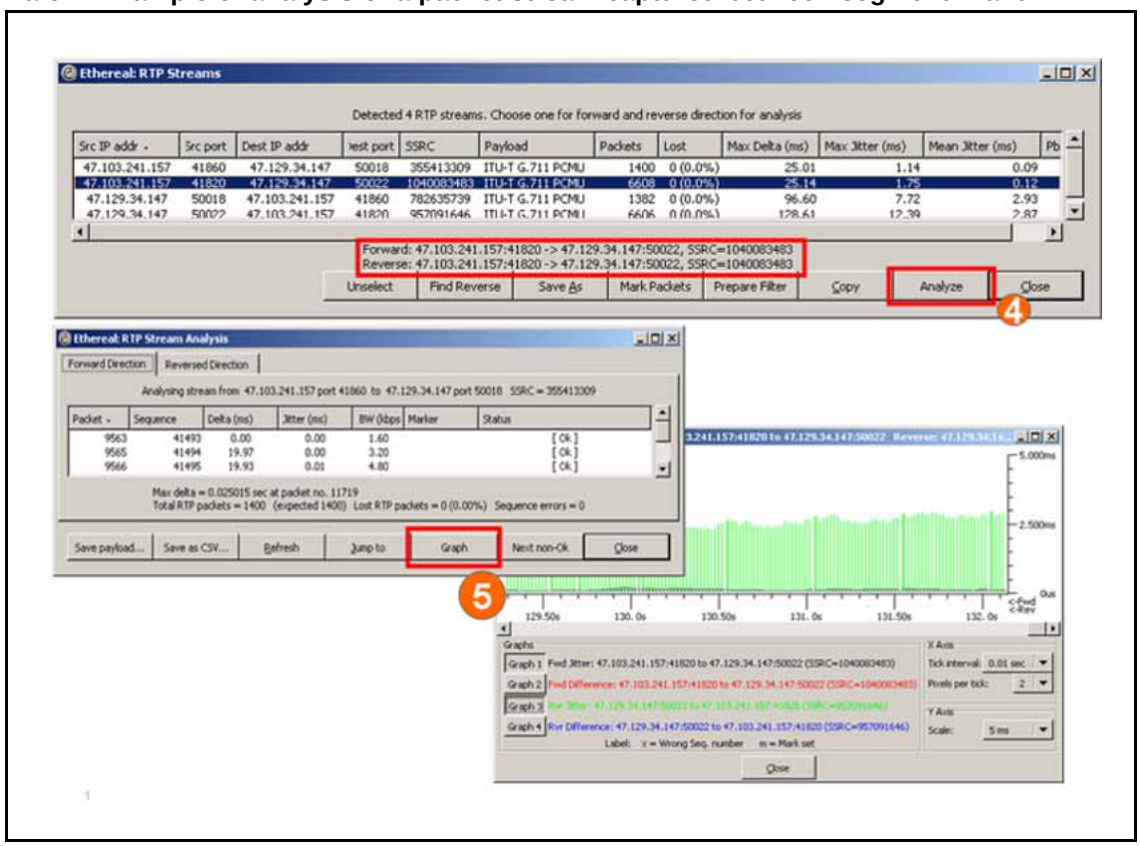
For an example of packet stream analysis for jitter and packet loss, see Figure 16 "Part 1: Example of analysis of a packet stream captured between segment A and B" (page 65) and Figure 17 "Part 2: Example of analysis of a packet stream captured between segment A and B" (page 66).

Figure 16
Part 1: Example of analysis of a packet stream captured between segment A and B


MCS-RTP.apc - Ethereal
File Edit View Go Capture Analyze Statistics Help
Summary
Protocol Hierarchy
Conversations
Endpoints
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANSI
Fax T38 Analysis...
GSM
H.225...
MTP3
RTP
SCTP
SIP...
Show All Streams
Stream Analysis...
Filter: rtp
Expression...
No. Time Source Protocol
9565 120.734225 47.103.241 RTP
9566 120.754154 47.103.241 RTP
9567 120.774232 47.103.241 RTP
9568 120.794170 47.103.241 RTP
Frame 9563 (214 bytes on w
Ethereal: RTP Streams
Detected 4 RTP streams. Choose one for forward and reverse direction for analysis
Src IP addr Src port Dest IP addr Dest port SSRC Payload Packets Lost Max Delta (ms) Max Jitter (ms) Mean Jitter (ms)
47.103.241.157 41860 47.129.34.147 50018 355413309 ITU-T G.711 PCMU 1400 0 (0.0%) 25.01 1.14 0.09
47.103.241.157 41820 47.129.34.147 50022 1040083483 ITU-T G.711 PCMU 6608 0 (0.0%) 25.14 1.75 0.12
47.129.34.147 50018 47.103.241.157 41860 782635739 ITU-T G.711 PCMU 1382 0 (0.0%) 96.60 7.72 2.93
Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button
Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

Copyright © 2004–2008 Nortel Networks

Figure 17
Part 2: Example of analysis of a packet stream captured between segment A and B



Usually the WLAN IP Telephony Manager 2245 is placed in the same subnet as WLAN handsets. This was previously a rule, but it is now just a recommendation. The WLAN IP Telephony Manager 2245 sometimes must be placed in a different subnet from the handsets. However, the rules for delay, jitter, and packet loss still apply.

Ethernet connectivity between the WLAN IP Telephony Manager 2245 and the call server, or other voice endpoint, must never exceed 100 milliseconds (ms) of one-way delay, 30 ms of jitter, and 2% packet loss end to end regardless of the physical properties of the link. Whether the WLAN IP Telephony Manager 2245 is in the same subnet with handsets, the link between the WLAN IP Telephony Manager 2245 and the handset must be under 100 ms of one-way delay, 1 ms of jitter and under 2% packet loss.

WLAN Application Gateway 2246 planning

The optional WLAN Application Gateway 2246 requires a 10 Mbs half-duplex switched Ethernet connection.

Copyright © 2004–2008 Nortel Networks

WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 installation requirements

Locate the WLAN IP Telephony Manager 2245 and optional WLAN Application Gateway 2246 in a space with:

- sufficient backboard mounting space and proximity to the LAN access device (switched Ethernet switch), Call Server, and power source
- rack-mount unit (if using)
- easy access to the front panel, which is used for cabling
- for the WLAN Application Telephony Gateway 2246, a maximum distance of 325 feet (100 meters) from the Ethernet switch
- for the WLAN IP Telephony Manager 2245, a maximum distance of 325 feet (100 meters) from the Ethernet switch

IP address planning

The WLAN IP Telephony Manager 2245, the optional WLAN Application Gateway 2246, and each of the wireless handsets and APs associated with them, requires an IP address.

ATTENTION
IMPORTANT!
If using DHCP for the rest of the network, the DHCP Server must have the static IP address of the WLAN IP Telephony Manager 2245 configured on it. If using DNS, the DNS Server must have the static IP address of the WLAN IP Telephony Manager 2245 configured on it.

The wireless handsets can be configured to use DHCP or can be assigned a static IP address . If there is no DHCP Server, the system administrator must determine what IP addresses are to be used for static addressing. As well, whether static IP addressing or DHCP is used, a pool of alias IP addresses must be configured on the WLAN IP Telephony Manager for the use of the wireless handsets. Ensure that the pool of alias IP addresses is reserved exclusively for the use of the wireless handsets.

For information about configuring a static IP address on a WLAN IP Telephony Manager 2245, see “WLAN IP Telephony Manager 2245 configuration” (page 93). For information about configuring a static IP address for a WLAN Application Gateway 2246, see “Configuring the WLAN Application Gateway 2246 IP address” (page 146). For information about configuring a static IP address on the handsets, see *WLAN Handsets Fundamentals (NN43001-505)*, . For information about assigning IP addresses to the APs, see the vendor-specific documentation.

Record the static IP address assignments and store them in a safe place.

Copyright © 2004–2008 Nortel Networks

IP addressing with DHCP

A pool of alias IP addresses must be configured on the WLAN IP Telephony Manager 2245 for the use of the wireless handsets. The use of a 22-bit subnet mask provides IP addresses for approximately 500 wireless handsets (1024 nodes). Allocate a pool of an equal number of IP addresses on the DHCP server for the wireless handsets.

For example:

142.223.204.1 to 142.223.205.254 are allocated on the DHCP Server for the use of the wireless handsets.

142.223.206.1 to 142.223.207.254 are configured on the WLAN IP Telephony Manager for IP aliases for the wireless handsets.

Ensure that all these IP addresses are reserved on the DHCP Server for the use of the wireless handsets and not assigned to any other device.

Planning worksheets

Complete this worksheet and the worksheet in Table 7 "Wireless handset planning worksheet" (page 69) before beginning the installation.

Copy and complete this worksheet in Table 6 "WLAN IP Telephony Manager 2245 planning worksheet" (page 68) for each WLAN IP Telephony Manager 2245. Obtain the necessary information from the network administrator.

Table 6
WLAN IP Telephony Manager 2245 planning worksheet

Unit number	
IP address	
Hostname	
Subnet Mask	
Default Gateway	
WLAN IP Telephony Manager 2245	
TFTP Download Master IP address	
DNS Server	
DNS Domain	
WINS Server IP address	
Workgroup name	
Syslog Server IP address	

Copyright © 2004–2008 Nortel Networks

Table 6
WLAN IP Telephony Manager 2245 planning worksheet (cont'd.)

First alias IP address	
Last alias IP address	

Copy and complete the worksheet from Table 7 "Wireless handset planning worksheet" (page 69) to maintain a configuration record for the handsets.

Table 7
Wireless handset planning worksheet

Line *	MAC Address *	User Name	Dialing Ext.	IP Address (if statically configured)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
***—required only if using the optional WLAN Application Gateway 2246.**				

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

System information

This chapter contains information about the following topics:

- “Bandwidth management” (page 71)
- “Codecs” (page 73)
- “Jitter buffer” (page 74)
- “RLR and SLR” (page 74)
- “RTCP” (page 74)
- “Gain adjustment” (page 75)
- “Programmable rings and tones” (page 75)
- “Virtual Office” (page 75)
- “Branch Office” (page 75)
- “Survivable Remote Gateway” (page 76)
- “External Applications Server” (page 77)
- “End-to-end QoS” (page 77)
- “NAT” (page 77)
- “CS 1000 features” (page 84)
- “IP Phone 2004 features” (page 84)

Bandwidth management

The existing CS 1000 Release 5.0 software bandwidth management mechanism using bandwidth zones applies to the handsets.

Zones

A WLAN IP Telephony Manager 2245 group consists of a 0 to 15 WLAN IP Telephony Manager 2245 units, and their associated wireless handsets.

Copyright © 2004–2008 Nortel Networks

It is good practice to create a Bandwidth Management Zone for each WLAN IP Telephony Manager 2245 group (one group per subnet) in LD 117. Use the **CHG ZDES** command to name the zone with the IP address of the WLAN IP Telephony Manager 2245.

```
=> NEW ZONE <zone number>

=> CHG ZDES <zone number> <Wnnn.nnn.nnn.nnn>
```

where

W indicates WLAN IP Telephony Manager 2245 and **nnn.nnn.nnn.nnn** is the IP address of the WLAN IP Telephony Manager 2245.

```
=> PRT ZDES ALL
```

This allows the system administrator or support personnel to print a list of the IP addresses of all the WLAN IP Telephony Manager 2245 units in the system simply by printing the Zone designators in LD 117. They are printed as Wnnn.nnn.nnn.nnn. This enables support personnel to easily obtain the IP address of a WLAN IP Telephony Manager 2245 so they can telnet to the WLAN IP Telephony Manager 2245 in order to diagnose and correct problems.

Zones for wireless handsets

Assign the virtual line TNs for the wireless handsets (configured in LD 11) to the zone number assigned to its home WLAN IP Telephony Manager 2245 group. Using LD 117, this enables support personnel to list the current registration status of all wireless handsets that belong to the zone of a specific WLAN IP Telephony Manager 2245 group.

```
=> STIP ZONE <zone number>
```

All wireless handsets currently registered (checked in) with their home WLAN IP Telephony Manager 2245 group is listed. The format of the list is **TERMIP = <alias IP address>** . Any wireless handsets that are currently checked in with another WLAN IP Telephony Manager 2245 group are listed with a TERMIP in a different subnet from that of their home WLAN IP Telephony Manager 2245 group ZDES.

Current registration status of wireless handsets

To list the current registration status of all wireless handsets that are registered in a specific subnet, regardless of their home zone, use either of the following LD 117 commands.

```
STIP TERMIP <subnet of the WLAN IP Telephony Manager 2245 group>
```

OR

```
PRT IPDN <subnet of the WLAN IP Telephony Manager 2245 group>
```


Copyright © 2004–2008 Nortel Networks

Alias IP address

Using the DN of a wireless handset, support personnel can obtain the current or most recent alias IP address used by a wireless handset when it checked in with a WLAN IP Telephony Manager 2245 group, and subsequently registered with the LTPS and Call Server.

```
=> PRT DNIP <DN of wireless handset>
```

Wireless telephone type designation

Unless there is another preferred use for the DES (Designator) prompt in LD 11, Nortel recommends using the DES prompt to indicate the type of WLAN Handset—either type 2210, 2211, 2212, or 6120—for the 2004P1 or the 2004P2 type of virtual line TN. This allows support personnel to enter 2210, 2211, 2212 or 6120 at the LD 20 DES prompt and receive a list of handsets that are configured on the Call Server.

Call blocking

The WLAN IP Telephony Manager 2245 controls the media stream and blocks calls due to bandwidth constraints on any AP without notifying the Call Server.

- The WLAN IP Telephony Manager 2245 can be configured with the maximum number of simultaneous calls allowed on a single AP.
- On an incoming call for a wireless handset associated with a full AP, the caller hears ringback and the Call Forward No Answer (CFNA) treatment is applied, such as forwarding the call to voice mail. The called party is not notified of the incoming call.
- If the call originates from a wireless handset that is on a bandwidth-restricted AP, the caller hears a warning tone and the call is blocked.
- If a wireless handset moves into an area serviced by an AP that is already at capacity, the wireless handset does not associate with the new AP. Instead, the wireless handset attempts to remain associated with an AP that has sufficient bandwidth. This could result in packet loss, degraded signal and voice quality, and a call could be dropped.
- UNIStim signaling, such as watchdog updates or lamp audit, are not affected by the bandwidth constraint.

Codecs

G.711, G.729A, and G.729B codecs are supported. The RTP packets that transit between the wireless handsets and the WLAN IP Telephony Manager 2245 always contain 30 ms of voice. The WLAN IP Telephony

Copyright © 2004–2008 Nortel Networks

Manager 2245 repackages the voice data to the correct packet size. The jitter buffer is always configured to 70 ms, and any UNIStim messages that configure the jitter buffer are ignored.

ATTENTION
IMPORTANT!
If the wireless handset is registered to the same LTPS as the IP Phones, configure only the subset of codecs supported by both the wireless handsets and the IP Phones.

If it is necessary for the IP Phone to use a codec that is not supported on the wireless handsets, such as G.723.1, the wireless handsets must be configured on their own separate node.

If a remote endpoint is configured for G.723.1 as the Best Bandwidth (BB) Codec and G.711 as the Best Quality (BQ) Codec, (G.729 is not configured), the media path negotiates to G.711. The result can be unexpected consequences on a narrow-band link.

Jitter buffer

The handsets do not support a configurable jitter buffer. If they receive the Jitter Buffer Configuration UNIStim message, the command is ignored. The jitter buffer is fixed at 70 ms.

There are two implications of a fixed jitter buffer setting:

- If the system jitter buffer setting is less than 70 ms (default is 50 ms), there is a slightly longer delay in the IP Phone receive direction.
- If the system jitter buffer setting is longer than 70 ms to accommodate severe network jitter, there could be slightly higher packet loss in the IP Phone receive direction.

The longer than normal jitter buffer setting is reasonable since extra jitter is introduced by the RF portion of the link.

RLR and SLR

The handsets do not support UNIStim messages used to adjust the Receive Loudness Rating (RLR) and Send Loudness Rating (SLR) of the wireless handset.

RTCP

Handsets do not support Real-time Transport Control Protocol (RTCP). Incoming RTCP packets sent to the wireless handsets are actually sent to the WLAN IP Telephony Manager 2245 and are discarded. If the wireless handset is queried for RTCP parameters, the wireless handset returns dummy values of 0 jitter, 0 latency, and 0 packet loss.

Copyright © 2004–2008 Nortel Networks

Gain adjustment

The handsets ignore any UNIStim messages that adjust the loss plan of the wireless handset.

Programmable rings and tones

The wireless handsets support alerting cadences but only a single alerting frequency.

The wireless handsets have the same call progress tone capability as the existing IP Phones 2004.

In/Out of Service tones

When the handset completes registration with the Call Server, it plays the In Service tone. When the handset loses connection with the Call Server and resets, it plays the Out of Service tone.

Virtual Office

The handsets support Virtual Office. For more information, see *Features and Services Fundamentals (NN43001-106)*, and *IP Line Fundamentals (NN43001-500)*, .

Branch Office

The handsets are supported in a branch office location using the Branch Office feature. Branch Office refers to the Media Gateway 1000B and the Survivable Remote Gateway (SRG). A WLAN IP Telephony Manager 2245 and supported APs must be installed at the branch office location. Branch office wireless handsets do not require wireless handset infrastructure in the main office.

The wireless handsets in a branch office configuration behave like an IP Phone 2004 in the Branch Office feature. The wireless handsets are administered in the same manner as the IP Phone 2004. The display on the wireless handsets is almost the same as the display on the IP Phone 2004, with one exception—the Local mode display.

Local mode display

The default state of the wireless handset is Standby. To determine whether the wireless handset is in Local mode, press the off-hook (Green) or the MENU keys on the WLAN Handset 2210/2211/2212 or the soft keys and the Nav keys on the WLAN Handset 6120/6140. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting the handset in communication with the primary Signaling Server.

Copyright © 2004–2008 Nortel Networks

For the MG 1000B, if a wireless handset is registered to the Small System Controller (SSC) in Local mode, the local-mode license information appears on the wireless handset on the second line of the display. Since the maximum number of display characters on the wireless handset is 19 characters, the local-mode license information about the wireless handset display is truncated. See Table 8 "IP Phone 2004 and handset Local mode license display (MG 1000B only)" (page 76).

Table 8
IP Phone 2004 and handset Local mode license display (MG 1000B only)

IP Phone 2004	Handset
Licensed days left x	Licensed days lft x
Licensed days left xx	Licensed ds lft xx
Beyond licensed period	Beyond licensd prd

For more information about Branch Office, see *Branch Office Installation and Commissioning (NN43001-314)*, .

Survivable Remote Gateway

The handset can be deployed in a Survivable Remote Gateway (SRG) configuration for both SRG 1.0 and SRG50.

The handset supports Virtual Office in SRG for Normal mode. It is not supported in Local mode.

Test Local mode is not accessible because the Services key is not supported in Local mode.

The navigation keys are supported in Normal mode and not in Local mode.

Since the default state of the wireless handset is Standby, it is only possible to determine if the wireless handset is in Local mode by pressing the off-hook (Green) or MENU keys. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting it in communication with the primary Signaling Server in the main office.

ATTENTION
In order to allow SRG 1.0 systems based on BCM 3.6, to correctly operate with the handsets, they must have a software patch installed. The patch can be downloaded from the Nortel Electronic Software Delivery Web site.The BCMSRG 3.6 WLAN IP Telephony Feature patch is called BCM_360[1].039__WLAN_IP_Telephony_Patch.exe, which includes 51 files required for automated patch installation.

SRG 1.0 based on BCM 3.7 or SRG50 systems do not require a patch.

Copyright © 2004–2008 Nortel Networks

For more information about SRG, see *Main Office Configuration Guide for Survivable Remote Gateway 50 (NN43001-307)*, .

External Applications Server

The External Applications Server (XAS) applications are not available on the handsets.

End-to-end QoS

End-to-end QoS, such as DiffServ, and Layer 2 QoS, such as 802.1 Qp, are not supported on the wireless telephone system. Any UNIStim commands sent to the wireless handsets attempting to adjust Layer 2 or Layer 3 QoS parameters are ignored.

However, the WLAN IP Telephony Manager 2245 can tag packets with a Differentiated Services Code Point (DSCP) tag. For more information, see "Quality of Service" (page 170). You can also provide QoS mechanisms through the configuration of network equipment.

The Layer 2 switch port to which the WLAN IP Telephony Manager 2245 is connected can be configured to add 802.1 Qp tagging. The Layer 3 port that acts as the gateway for the WLAN IP Telephony Manager 2245 can be configured to add the appropriate DiffServ tagging. Since all of the signaling and media traffic passes through the WLAN IP Telephony Manager 2245, all packets are tagged with the appropriate priority. If more than one WLAN IP Telephony Manager 2245 is used, each Layer 2 port to which a WLAN IP Telephony Manager 2245 is connected must be configured to add the 802.1 Qp tagging.

NAT

Handsets can be deployed in an Network Address Translation (NAT) environment.

This section describes important considerations that must be taken into account when using the handsets in a NAT environment. Failure to comply with or heed these considerations can result in wireless handset malfunction.

For detailed information about NAT and the NAT Traversal feature, see *IP Line Fundamentals (NN43001-500)*, .

NAT Traversal feature

The NAT Traversal feature is used where the IP Phone (this includes the handsets) is located on the private side of the NAT router, while the rest of the Server resides on the public side.

Copyright © 2004–2008 Nortel Networks

To ensure correct deployment of the wireless handsets in this type of network configuration, most, if not all, of the WLAN equipment must reside on the private side of the NAT router.

Network configurations

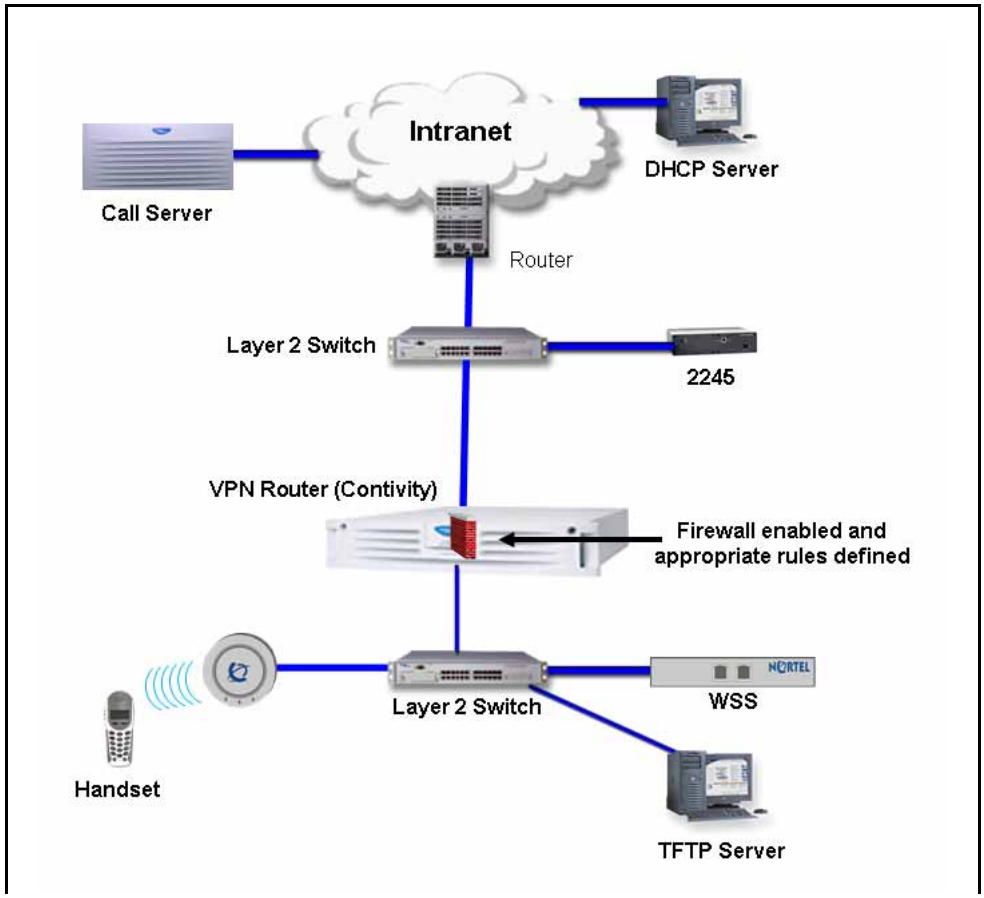
The WLAN Handset 2212 has a VPN feature that enables an IPsec tunnel to a Nortel VPN Router, which is the only IPsec platform supported today. This feature alters some of the usual design recommendations for the telephony components, such as the WLAN IP Telephony Manager 2245. Usually, the WLAN IP Telephony Manager 2245 is placed in the same subnet with the handsets.

With the VPN feature enabled, the WLAN IP Telephony Manager 2245 now resides behind the VPN Router in a different subnet from the handsets; however, even though the same-subnet restriction has been lifted, it is still very important to locate the WLAN IP Telephony Manager 2245 as close to the handsets as possible. In this case, it is located immediately behind the VPN Router (and in the same subnet as the VPN Router). The VPN Router must also be located as close to the handsets as possible.

You can deploy the handsets behind a NAT router with no Security Switch, as shown in Figure 18 "VPN design over a Layer 2 network" (page 79). This configuration includes a Layer 2 switch, which can be any Layer 2 switch (for example, Nortel Ethernet Switch 450). No Layer 3 device, such as a router, can be located between the wireless handsets and the WLAN IP Telephony Manager 2245.

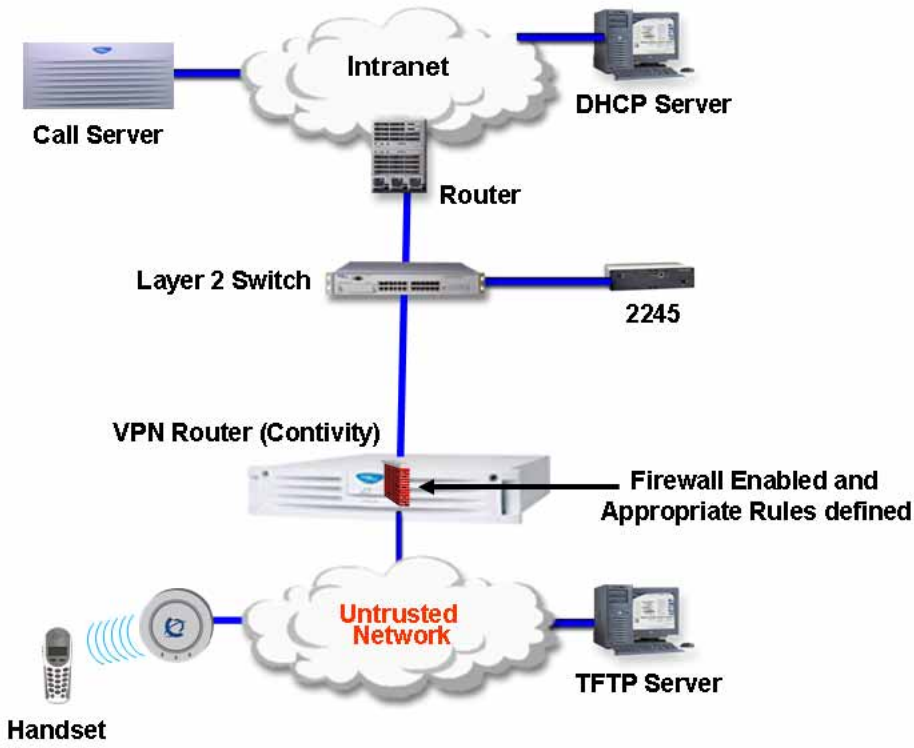
Copyright © 2004–2008 Nortel Networks

Figure 18
VPN design over a Layer 2 network



Copyright © 2004–2008 Nortel Networks

Figure 19
VPN design over a Layer 3 network



ATTENTION
If the WLAN IP Telephony Manager 2245 is not in the same subnet as the handsets, the handsets do not work.

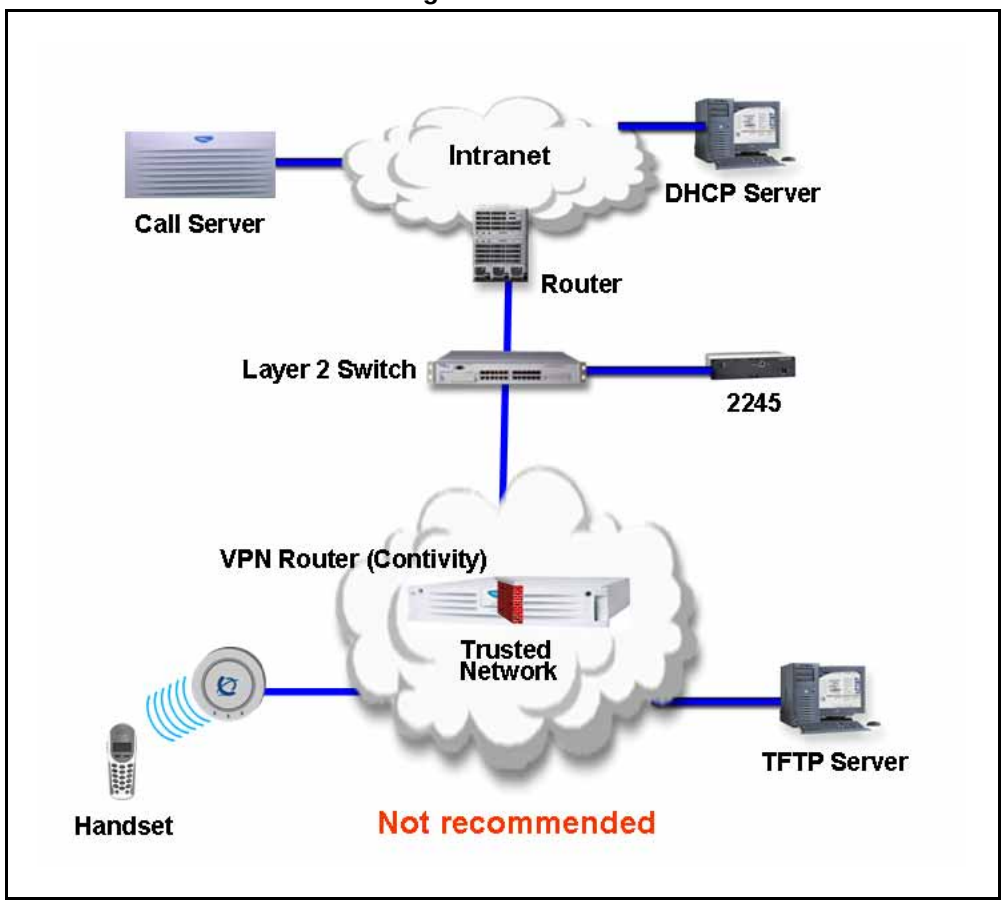
ATTENTION
In Figure 18 "VPN design over a Layer 2 network" (page 79), Figure 19 "VPN design over a Layer 3 network" (page 80), Figure 20 "Not recommended VoWLAN design" (page 81), and Figure 21 "Network configuration 3 with Full DHCP Server" (page 83), the clouds can represent a corporate intranet or the public Internet.

Make the VPN Router public interface the default gateway for the handsets, and if not the direct gateway for clients, at least ensure that traffic comes from the WLAN into the public interface, not the private interface.

Copyright © 2004–2008 Nortel Networks

Connect the private interface of the VPN Router to the trusted side of the network. Make sure that client DHCP traffic flows through the VPN Router. If a network path around the VPN Router exists for the handsets to get DHCP assignments, the routing requirements on the VPN Router become much more complicated. To support such a scenario, you must configure static routes on the public interface as well as inject those routes into the routing protocol on the private interface. Therefore, Nortel recommends that you do not use the network design shown in Figure 20 "Not recommended VoWLAN design" (page 81) as a design for the VPN feature.

Figure 20
Not recommended VoWLAN design



If you deploy the VPN feature of the WLAN Handset 2212 in a mixed network where WLAN Handsets 2211/2210s are also in use, the design recommendation becomes a little more complex. If you place a WLAN IP Telephony Manager in the subnet with the WLAN Handsets 2210/2211, and place a WLAN IP Telephony Manager in the subnet with the VPN Router to support the WLAN Handset 2212, admission control problems for the telephony WLAN can occur. Each WLAN IP Telephony Manager counts the number of their own devices placing calls over APs, but does

Copyright © 2004–2008 Nortel Networks

not count the number of calls controlled by the other WLAN IP Telephony Manager. This creates a blind spot for each device, and it is possible to oversubscribe an AP by up to 2:1. The best solution to this problem is to have the WLAN Handsets 2210/2211 handsets use the same WLAN IP Telephony Manager as the WLAN Handset 2212 (VPN). This WLAN IP Telephony Manager is on the other (remote) side of the VPN Router from the handsets, that is, over a routed hop.

WLAN IP Telephony Manager 2245 in a NAT environment

The IP Telephony Manager 2245 must be in constant communication with the handsets to ensure handset functionality. Since the IP Telephony Manager 2245 must be on the same subnet as the handsets, the IP Telephony Manager 2245 must be located on the private side of the NAT router. The wireless VoIP network does not function if the IP Telephony Manager 2245 is located on the public side of the NAT router.

Port 10000 is used for bidirectional UDP traffic between the handset alias IP addresses of the IP Telephony Manager 2245 and the Echo Server on the TPS used for NAT detection. Any network security devices that monitor network traffic between the IP Telephony Manager 2245 and the Signaling Server(s) must be configured to allow traffic using port 10000 to pass freely between these devices.

DHCP Server location in a NAT environment

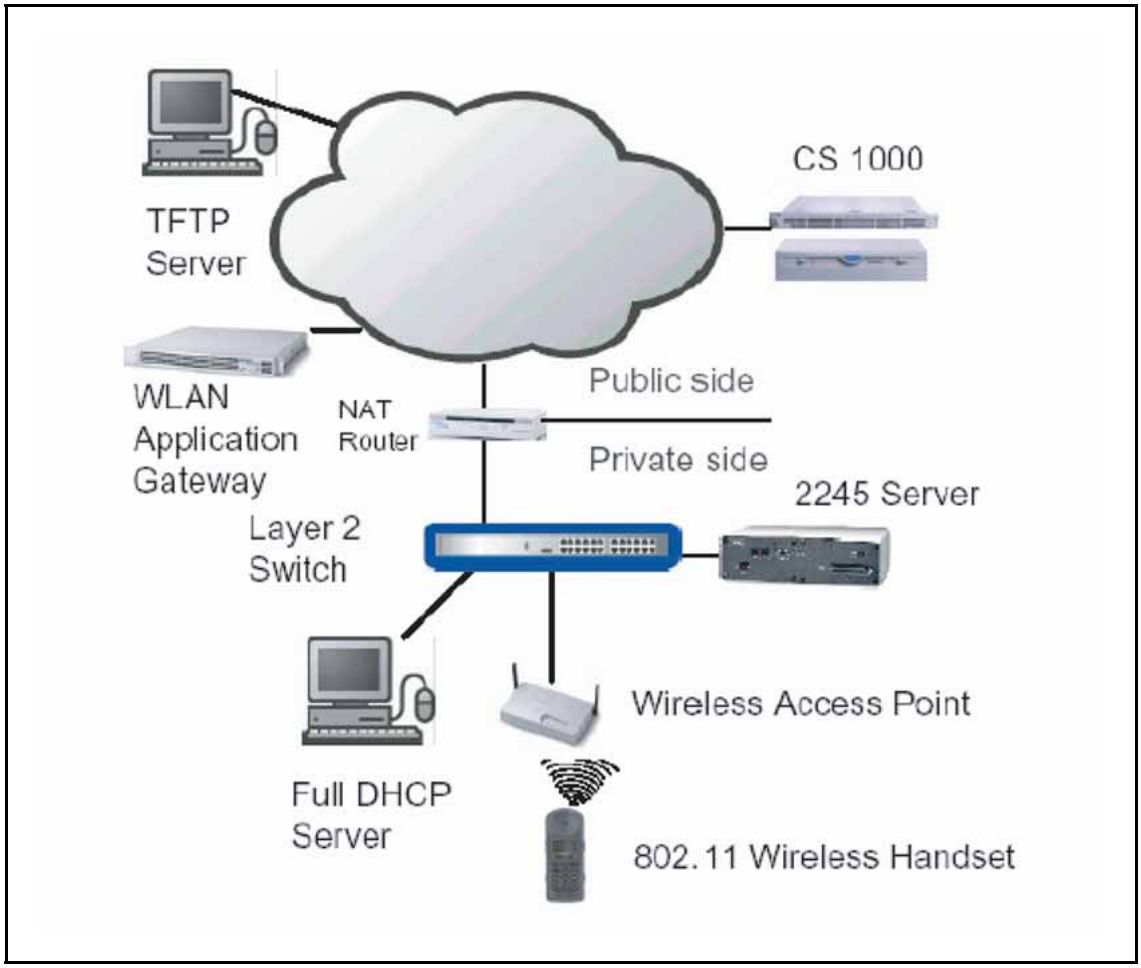
The WLAN Handsets only support Full DHCP. The device acting as a DHCP Server to the WLAN Handsets must be configurable to send the vendor-specific DHCP fields.

In some cases, the NAT router acts as the DHCP Server. In this case, configure the NAT router with the required DHCP parameters and necessary information.

If a separate DHCP Server is used, it must be located on the private side of the network. See Figure 21 "Network configuration 3 with Full DHCP Server" (page 83) for more information.

Copyright © 2004–2008 Nortel Networks

Figure 21
Network configuration 3 with Full DHCP Server



TFTP Server location in a NAT environment

The TFTP Server can be located on the public side of the network. In this case, the NAT router (and Wireless Security Switch if deployed) can have to be configured to allow WLAN Handsets access to the TFTP Server (allow traffic through on the required ports). This scenario is represented in Figure 21 "Network configuration 3 with Full DHCP Server" (page 83).

Another option is to place the TFTP Server on the private side of the network.

WLAN Application Gateway 2246 in a NAT environment

If a WLAN Application Gateway 2246 is to be deployed, the requirements are similar to that of the TFTP server.

Copyright © 2004–2008 Nortel Networks

The WLAN Application Gateway 2246 can be located on the public side of the network as long as traffic is allowed on the correct ports. This scenario is represented in Figure 21 "Network configuration 3 with Full DHCP Server" (page 83).

Alternatively, the WLAN Application Gateway 2246 can be placed on the private side of the network.

CS 1000 features

Nearly all CS 1000 features are supported on the wireless telephone system and WLAN Handsets 22x1. Partially supported features are listed in Table 9 "Partially supported CS 1000 features" (page 84). The features that are not supported are listed in Table 10 "CS 1000 not supported" (page 84).

Table 9
Partially supported CS 1000 features

Feature	Feature full name	Description
DIG	Dial Intercom Group	Handsfree call option is not supported.
HOT I	Intercom Hotline	Voice Intercom Hotline (default) is not supported. The Ringing option is supported.
RGA	Ring Again	Since the handsets cannot buzz, there is no Ring Again tone. The only way to use the Ring Again feature is to determine if the Ring Again indicator is flashing, which is possible only when the wireless handset is in the active state.

Table 10
CS 1000 not supported

Feature	Feature full name	Description
AAB	Automatic Answerback	Cannot automatically enable Handsfree.
VCC	Voice Call	Cannot automatically enable Handsfree.
	Active Call Failover	Not supported.

IP Phone 2004 features

Table 11 "IP Phone 2004 features" (page 85) provides information about the IP Phone 2004 features for the handsets.

Copyright © 2004–2008 Nortel Networks

Table 11
IP Phone 2004 features

Feature	Supported on the WLAN handsets	Description
Keypad	Yes	
Navigation keys	Yes	Up—Volume Up button Down—Volume Down button Left button— Right button—
6 feature keys	Yes	
4 soft-labelled keys	Yes	
Display	Partially	IP phone 2004: 5x24 display Handsets: 4x19 display
Message Waiting Indicator	Yes	Small envelope icon in the top right of the handset LCD display ✉
Branch Office	Yes	
Survivable Remote Gateway	Yes	
Virtual Office	Partially	No Services key. Use FCN+7 for the Services key to support Virtual Office.
XAS	No	No Expand key.
Personal Directory Callers List Redial List	Yes	

Copyright © 2004–2008 Nortel Networks

Table 11
IP Phone 2004 features (cont'd.)

Feature	Supported on the WLAN handsets	Description
Password Admin	No	The handsets can be password-protected, but this is different from the IP Phone 2004 password protection mechanism. The IP Phone 2004 password protection is supported, in addition to the handset password protection.
KEM	No	

Copyright © 2004–2008 Nortel Networks

Installation

This chapter contains information about the following topics:

- "Required materials" (page 87)
- "Preinstallation checklist" (page 88)
- "WLAN IP Telephony Manager 2245 installation tasks" (page 88)
- "WLAN Application Gateway 2246 installation" (page 91)

Required materials

The following equipment must be provided by the customer:

- power outlet(s)—must accept the provided AC adapter, one for the WLAN IP Telephony Manager 2245 and one for the WLAN Application Gateway 2246 (if used).
- plywood backboard space—the WLAN IP Telephony Manager 2245 is designed to be wall-mounted to 1/2 in. plywood securely screwed to the wall.
  OR
  optional WLAN IP Telephony Manager 2245 rack-mount kit (must be ordered separately), containing mounting plates and screws
- screws—used to mount the WLAN IP Telephony Manager 2245 to the wall. Four #8 - 1/2 in. pan-head wood screws (or similar devices) are required.
- 10BaseT CAT5 cable with an RJ-45 connector for the optional WLAN Application Gateway 2246—provides a connection to the Ethernet switch.
- CAT5 cable with an RJ-45 connector for the WLAN IP Telephony Manager 2245—provides a connection to the Ethernet switch.
- DB-9 female null-modem cable—required for initial configuration of the WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246.

Copyright © 2004–2008 Nortel Networks

Supplied equipment

Each WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 is shipped with one Class II AC adapter with 24V DC, 1A output.

Preinstallation checklist

Ensure that the following requirements are met prior to installation:

- The location chosen for the WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 is adequate and power is available.
- APs are SVP-compatible and coverage is adequate.
- A dedicated line is available for remote modem access, if needed.
- The telephone system administrator is on-site to program the existing telephone system.

WLAN IP Telephony Manager 2245 installation tasks

The following are the tasks that must be completed to install the WLAN IP Telephony Manager 2245:

1. “Wall-mount” (page 89).
or
“Rack-mount” (page 90).
2. “LAN connection” (page 91).
3. “Power connection” (page 91).

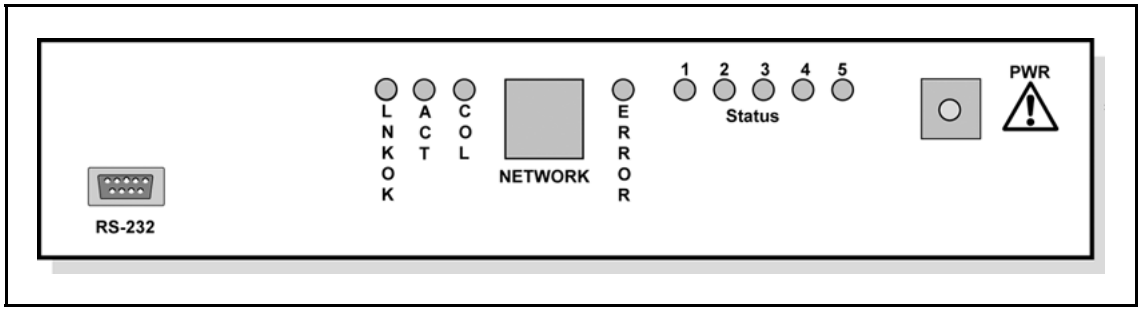
About the front panel

The front panel of the WLAN IP Telephony Manager 2245 contains ports to connect to the following:

- power
- LAN
- administrative computer through an RS-232 port
  Status LEDs supply information about status and activity of the WLAN IP Telephony Manager 2245. See Figure 22 "WLAN IP Telephony Manager 2245 front panel" (page 89).

Copyright © 2004–2008 Nortel Networks

Figure 22
WLAN IP Telephony Manager 2245 front panel



- **RS-232** port—the male DB-9 connector (DTE). Provides an RS-232 connection to a terminal, terminal emulator, or modem for system administration.
- Link LEDs
  - **LNKOK**—lit when there is a network connection
  - **ACT**—lit when there is system activity
  - **COL**—lit if there are network collisions
- **NETWORK**—connects the WLAN IP Telephony Manager 2245 to the wired Ethernet LAN
- **ERROR LED**—lit when the system has detected an error
- **Status** LEDs—indicate system error messages and status
  - **1**—heartbeat
  - **2**—active calls
  - **3, 4, 5**—currently unused
- PWR—connects to the AC adapter supplying power to the system

WARNING
Use only the provided Class II AC adapter with 24V DC, 1A output.

Wall-mount

The WLAN IP Telephony Manager 2245 can be mounted either vertically or horizontally.

Copyright © 2004–2008 Nortel Networks

Procedure 2
Wall-mounting the WLAN IP Telephony Manager 2245

Step	Action
1	Use a 18-inch drill bit to drill four pilot holes, on 1.84 by 12.1 inch centers (approximately equivalent to 1-1316 inch by 12-18 inch).
2	Insert the #8 x 34-inch screws in the pilot holes and tighten, leaving a 18 to 14-inch gap from the wall.
3	Slide the WLAN IP Telephony Manager 2245 over the screws until the WLAN IP Telephony Manager 2245 drops into place in the keyhole openings of the flange.
4	Tighten screws fully.

--End--

Rack-mount

The rack-mount kit is designed for mounting the WLAN IP Telephony Manager 2245 in a standard 19-inch rack and contains the following equipment:

- Mounting plates—two for each WLAN IP Telephony Manager 2245 to be mounted.
- Screws—four rack-mount screws for each WLAN IP Telephony Manager 2245 to be mounted.

Follow the steps in Procedure 3 “Rack-mounting the WLAN IP Telephony Manager 2245” (page 90) to rack-mount the WLAN IP Telephony Manager 2245.

Procedure 3
Rack-mounting the WLAN IP Telephony Manager 2245

Step	Action
1	Remove the corner screws from the WLAN IP Telephony Manager 2245.
2	Screw the U-shaped end (round screw holes) of the two mounting plates to the WLAN IP Telephony Manager 2245.
3	Screw the other end of the two mounting plates (oblong screw holes) to the rack.
4	Repeat steps 1-3 for each additional WLAN IP Telephony Manager 2245. The mounting plate is designed to provide

Copyright © 2004–2008 Nortel Networks

the correct minimum spacing between units. When mounting multiple units, stack the units in the rack as closely as possible.

--End--

LAN connection

Use an RJ-45 cable to connect the **NETWORK** port on the WLAN IP Telephony Manager 2245 to the connecting port on the Ethernet switch.

Power connection

Follow the steps in Procedure 4 "Connecting the power" (page 91) to connect the power to the WLAN IP Telephony Manager 2245.

Procedure 4
Connecting the power

Step	Action
1	Connect the power plug from the AC adapter to the jack labeled PWR on the WLAN IP Telephony Manager 2245.

WARNING
Use only the provided Class II AC adapter with output 24V DC, 1A.

2	Plug the AC adapter into a 110V AC outlet to supply power to the WLAN IP Telephony Manager 2245. The system cycles through diagnostic testing and the LEDs blink for approximately one minute.
3	When the system is ready for use, verify the following: **a** **ERROR** LED is off. **b** **Status 1** is blinking.

--End--

WLAN Application Gateway 2246 installation

For information about installing the optional WLAN Application Gateway 2246, see "WLAN Application Gateway 2246" (page 141).

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

WLAN IP Telephony Manager 2245 configuration

This chapter contains information about the following topics:

- "Introduction" (page 93)
- "Configuration tasks" (page 95)
- "Connect to the WLAN IP Telephony Manager 2245" (page 95)
- "Configure the network" (page 97)
- "Configure the WLAN IP Telephony Manager 2245" (page 100)
- "Change the password" (page 102)

Introduction

The WLAN IP Telephony Manager 2245 acts as a proxy for the wireless handsets and provides several services for them. It is connected to the same subnet as the wireless handsets. The wireless handsets always communicate voice and signaling directly with the WLAN IP Telephony Manager 2245, using the proprietary SpectraLink Voice Protocol (SVP).

SVP is required for quality of service (QoS) because the current IEEE 802.11a/b/g wireless LAN standard provides no mechanism for differentiating audio packets from data packets. This standard is undergoing revision to version 802.11e to provide functionality in an industry standard similar to SVP, therefore ensuring high-quality voice in a mixed-client environment.

The wireless handsets are configured with the IP address of a designated WLAN Telephony Manager 2245. As the wireless handsets register, they receive a list of IP addresses of other WLAN Telephony Manager 2245 in the network and they distribute among other WLAN Telephony Manager 2245 to share the load. This WLAN Telephony Manager 2245 becomes the registration point. The list of addresses automatically updates each time the wireless handset powers on.

Copyright © 2004–2008 Nortel Networks

If the WLAN Telephony Manager 2245 fails, the wireless handset drops active calls, then re-registers with another WLAN IP Telephony Manager 2245 in their list. The wireless handsets return to active state after this registration period. This failure does not affect other wireless handsets registered on the other WLAN IP Telephony Manager 2245 units.

The recovery period for the wireless handsets on the failed WLAN IP Telephony Manager 2245 is approximately 60 seconds.

The entire network is inoperative when new software downloads to the network of WLAN IP Telephony Manager 2245 units. When the download completes, the network comes back into service automatically.

This functionality requires the minimum software. See Table 12 "Minimum software requirements" (page 94).

Table 12
Minimum software requirements

Device	Minimum version
WLAN IP Telephony Manager 2245	174.034
WLAN Handset 2210/2211/2212	97.071
WLAN Handset 6120/6140	115.015

If either component is at an earlier release then the system works in the current master or slave mode.

Functional description

The WLAN IP Telephony Manager 2245 provides the following services to the handsets:

- It acts as a proxy for every wireless handset; that is, all UNIStim signaling and RTP media to and from the wireless handset pass through the WLAN IP Telephony Manager 2245. Except for the initial DHCP and TFTP sessions, the wireless handsets only communicate with the WLAN IP Telephony Manager 2245.
- The WLAN IP Telephony Manager 2245 server tags and untags packets with the SVP header. SVP packets have the protocol byte of the IP header configured to 0x77. SVP-compliant APs use this proprietary tagging to give priority to tagged packets. For UDP (UNIStim and RTP) packets going from the wireless handset to the network, the WLAN IP Telephony Manager 2245 replaces the SVP protocol number, 0x77, with the UDP number, 0x11. For packets going from the network to the wireless handset, the protocol number is changed from 0x11 to 0x77.
  Because the packets that traverse the network between the wireless handset and the WLAN IP Telephony Manager 2245 are not standard

Copyright © 2004–2008 Nortel Networks

IP packets (the packets use a nonstandard protocol number), there can be no Layer 3 routing in the path. Therefore, the wireless handsets and WLAN IP Telephony Manager 2245 units must be in the same logical subnet.

- RTP packets between the wireless telephone and the WLAN IP Telephony Manager 2245 always contain 30 ms worth of voice, no matter what is configured on the Call Server. The WLAN IP Telephony Manager 2245 repackages the RTP packets to conform to the size that is configured in the Call Server. This provides more efficient use of the available Radio Frequency (RF) bandwidth at the expense of slightly increased jitter and latency.
- The WLAN IP Telephony Manager 2245 is configured with a maximum allowable number of simultaneous media streams on a single AP. The WLAN IP Telephony Manager 2245 keeps track of the number of media streams on each AP and blocks calls to and from a wireless handset that would exceed the configured capacity. For more information about call blocking, see "Call blocking" (page 73).

A keep-alive packet exchange runs between the wireless handset and the WLAN IP Telephony Manager 2245 every 30 seconds. If the wireless handset detects that the WLAN IP Telephony Manager 2245 is unreachable, the wireless handset resets itself and attempts to reestablish a connection with other WLAN IP Telephony Manager 2245 units.

Configuration tasks

The following are the tasks required to configure the WLAN IP Telephony Manager 2245:

1. "Connect to the WLAN IP Telephony Manager 2245" (page 95).
2. "Configure the network" (page 97).
3. "Configure the WLAN IP Telephony Manager 2245" (page 100).
4. "Change the password" (page 102).

In the initial configuration of the WLAN IP Telephony Manager 2245, the IP addresses and the maximum number of active calls per AP must be configured. Later, you can use Telnet to configure the IP address of the TFTP Server where the software files are located and the hostname.

Connect to the WLAN IP Telephony Manager 2245

The initial connection to the WLAN IP Telephony Manager 2245 must be made through a serial connection to establish the WLAN IP Telephony Manager 2245 IP address. After the IP address is established, connection to the WLAN IP Telephony Manager 2245 can be done through the network using Telnet.

Copyright © 2004–2008 Nortel Networks

Nortel recommends that you perform the complete initial configuration after the serial connection is made.

Serial port connection

Follow the steps in Procedure 5 “Connecting to the WLAN IP Telephony Manager 2245 through a serial port” (page 96) to connect to the WLAN IP Telephony Manager 2245 through a serial port.

Procedure 5
Connecting to the WLAN IP Telephony Manager 2245 through a serial port

Step	Action
1	Using a DB-9 female, null-modem cable, connect the WLAN IP Telephony Manager 2245 to the serial port of a terminal or PC.
2	Run a terminal emulation program (such as HyperTerminal), or use a VT-100 terminal with the following configuration: • Bits per second: 9600 • Data bits: 8 • Parity: None • Stop bits: 1 • Flow control: None
	ATTENTION If you use Windows 2000, you must install Service Pack 2 to enable the use of HyperTerminal™.
3	Press **Enter** to display the login screen.
4	Enter the default login **admin** and the default password **admin**. The login name and password are case-sensitive. The **NetLink SVP-II System** screen appears.

--End--

Telnet connection

The Telnet method of connection is used for routine maintenance of the WLAN IP Telephony Manager 2245 for local and remote administration, depending on the network.

ATTENTION
You can only use Telnet after you configure the WLAN IP Telephony Manager 2245 IP address.

Copyright © 2004–2008 Nortel Networks

Follow the steps in Procedure 6 “Connecting to the WLAN IP Telephony Manager 2245 through Telnet” (page 97) to connect to the WLAN IP Telephony Manager 2245 through Telnet.

Procedure 6
Connecting to the WLAN IP Telephony Manager 2245 through Telnet

Step	Action
1	Run a Telnet session to the IP address of the WLAN IP Telephony Manager 2245.
2	Enter the login and the password. The login name and password are case-sensitive. The **NetLink SVP-II System** menu appears. The following menu choices are available: • **System Status**—view software code version, error messages, and status of operation. See “View software version” (page 106) and “Troubleshooting” (page 113). • **SVP-II Configuration**—set the mode and reset the system. See “Configure the WLAN IP Telephony Manager 2245” (page 100). • **Network Configuration**—set network configuration options, including IP addresses and hostname. See “Configure the network” (page 97). • **Change Password**—change the password for WLAN IP Telephony Manager. See “Change the password” (page 102). • **Exit**—exit the menu.

--End--

Configure the network

Select **Network Configuration** on the **NetLink SVP-II System** screen to configure the IP address and other network settings of the WLAN IP Telephony Manager 2245. An optional Hostname and the IP address of TFTP Server containing the software update files are also configured here.

Copyright © 2004–2008 Nortel Networks

Configure the following Network Configuration screen fields with information provided by the network administrator:

- **IP Address:**—enter the complete IP address for the WLAN IP Telephony Manager 2245, including digits and periods.

- **Hostname:**—optional field. Change the default hostname of this WLAN IP Telephony Manager 2245, if desired. Hostname is for identification purposes only. Do not include spaces.

- **Subnet mask**—the subnet mask of the subnet.
- **Default Gateway**—the default gateway for the subnet.
- **SVP-II TFTP Download Master**—the IP address of the TFTP Server where the software update files are saved. Enter one of the following:
  - NONE—disables this function
  - IP address of the TFTP Server that transfers software updates to the WLAN IP Telephony Manager 2245
- **DNS Server and DNS Domain**—used to configure Domain Name Services (DNS). Obtain the settings from the network administrator. Optionally, enter DHCP. This enables the DHCP client in the WLAN IP Telephony Manager 2245 to attempt to automatically obtain a valid IP address from the DHCP Server. The DHCP setting is only valid when the IP address is obtained from DHCP.
- **WINS Server**—the IP address of the Windows Name Services (WINS) Server. Obtain the settings from the network administrator. Optionally, enter DHCP. This enables the DHCP client in the WLAN IP Telephony Manager 2245 to attempt to automatically obtain a valid IP address from the DHCP Server. The DHCP setting is only valid when the IP address is obtained from DHCP.
  When WINS is configured, the WLAN IP Telephony Manager 2245 can translate hostnames to IP addresses. This means that when using Telnet, the WLAN IP Telephony Manager 2245 can be accessed using its hostname rather than its IP address.
- **Workgroup**—indicates whether a workgroup is configured in the WINS Server.
- **Syslog Server**—the IP address of the server where the system logs for the WLAN IP Telephony Manager 2245 are written. If a Syslog Server is configured, a message is sent to the Syslog Server when an alarm is generated. Enter one of the following:
  - NONE—disables this function
  - IP address of the Syslog Server

Copyright © 2004–2008 Nortel Networks

- **Maintenance Lock**—indicates whether the WLAN IP Telephony Manager 2245 is in Maintenance Lock mode.
- **Disable Telnet Service**—indicates whether a Telnet session can access the WLAN IP Telephony Manager 2245. The available options are:
  - **Y**—prevents a Telnet session from accessing the WLAN IP Telephony Manager 2245.
  - **N**—allows a Telnet session to access the WLAN IP Telephony Manager 2245.
- **Send/All**—in a system with multiple WLAN IP Telephony Manager 2245 units, the SendAll option is provided to speed configuration and ensure identical settings. The S=SendAll option enables configuration parameters of the selected field to be sent to every WLAN IP Telephony Manager 2245 on the LAN. SendAll can only be used after the IP address is configured on each WLAN IP Telephony Manager 2245 using a serial connection. If identical configuration parameters are to be used for all WLAN IP Telephony Manager 2245 units, configure only the IP address and custom hostname (if desired) on each WLAN IP Telephony Manager 2245 using the initial serial connection. Then connect through the LAN to this WLAN IP Telephony Manager 2245 and use SendAll to transmit identical configuration options of each field for all WLAN IP Telephony Manager 2245 units.

ATTENTION
IMPORTANT!
If SendAll is used on the system, all passwords must be identical. Do not change the password at the initial configuration if the SendAll option is used. Use the default password and change it globally, if desired, after a LAN connection is established for all WLAN IP Telephony 2245 units.

If independent administration of each WLAN IP Telephony Manager 2245 is desired, the passwords can be set during initial configuration.

Save the configuration

Reset the WLAN IP Telephony Manager 2245 in order to save the configuration parameters. Follow the steps in Procedure 7 “Saving the configuration” (page 99) to save the configuration.

Procedure 7
Saving the configuration

Step	Action
1	Press **Esc** on the keyboard.

Copyright © 2004–2008 Nortel Networks

If the WLAN IP Telephony Manager 2245 is in **Maintenance Lock**, a prompt appears asking if the configuration is to be saved.

2 Enter **Y**.

3 Alternatively, select the **Reset** option found in the **SVP-II Configuration** screen. Press **Esc**. See "Configure the WLAN IP Telephony Manager 2245" (page 100).

--End--

Configure the WLAN IP Telephony Manager 2245

The WLAN IP Telephony Manager 2245 is configured on the **SVP-II Configuration** screen where the mode of the WLAN IP Telephony Manager 2245 is configured. This screen is also used to lock the WLAN IP Telephony Manager 2245 for maintenance and reset the WLAN IP Telephony Manager 2245 after maintenance.

The WLAN IP Telephony Manager 2245 automatically locks for maintenance if the IP address is changed. When a Maintenance Lock occurs, the WLAN IP Telephony Manager 2245 must be reset upon exit. All active calls are terminated during a reset.

Access the **SVP-II Configuration** screen from the **NetLink SVP-II System** menu. Scroll to **SVP-II Configuration** and press **Enter**.

Perform the desired SVP-II configuration.

- **Phones per Access Point**—enter the number of simultaneous calls supported for the AP type. AP specifications are described in "Compatible Access Points" (page 215).
- **802.11 Rate**—select Automatic to allow the wireless handset to determine its rate (up to 11Mbs). Select 1MB/2MB to limit the transmission rate between the wireless handsets and APs.
- **First Alias IP Address and Last Alias IP Address**—enter the range of IP addresses that this WLAN IP Telephony Manager 2245 can use when acting as a proxy for the wireless handsets.
  If you install multiple WLAN IP Telephony Manager 2245 units, you must configure a different range of IP addresses for each WLAN IP Telephony Manager 2245. Use the following formula to determine how many addresses to configure for each WLAN IP Telephony Manager 2245:
  (number of handsets / number of WLAN IP Telephony Manager 2245 units) + 30%

Copyright © 2004–2008 Nortel Networks

ATTENTION
All alias addresses must be on the same subnet as the WLAN IP Telephony Manager 2245. The IP addresses cannot be duplicated on other subnets or WLAN IP Telephony Manager 2245 units. There is no limit to the number of IP addresses that can be assigned, but the capacity of each WLAN IP Telephony Manager 2245 is 500 wireless handsets.

- **Ethernet link**—select **auto-negotiate** unless there is a need to specify the link speed.
- **System Locked**—use this option to take the system down for maintenance. The default is N (No). Select Y (Yes) to prevent any new calls from starting. Enter N to restore normal operation.
- **Maintenance Lock**—the system automatically sets this option to Y (Yes) after certain maintenance activities that require a reset are performed, such as changing the IP address. Maintenance Lock prevents any new calls from starting. This option cannot be changed. It is automatically set by the system. Reset the WLAN IP Telephony Manager 2245 at exit to clear Maintenance Lock.
- **Inactivity Timeout**—use this option to configure the number of minutes that the administrative module can be left unattended before the system closes it. This number can be from 1 to 100. If the number is 0, the administrative module does not close due to inactivity.
- **QoS Configuration**—use this option to configure decimal values, from 0 to 63 (default 4), for all classes of traffic.
  To ensure the system transmits voice packets efficiently and with minimal delay, you must configure the decimal value for voice packets higher than the value for data packets. The configurable classes are:
  - Administration—used for Telnet, TFTP and other administrative traffic. This class can have the lowest priority because it does not require voice quality.
  - WT (in call)—traffic requires voice quality. Configure this class with a higher priority than WT (standby).
  - WT (standby)—traffic requires voice quality. Configure this class with a lower priority than WT (in call).
  - RTP—traffic is audio traffic to IP PBX; it requires voice quality.
  - PBX—traffic is not audio traffic to the PBX; voice quality is not required.
  - Inter-SVP2— traffic requires voice quality. Configure this class with a priority equal to WT (in call).

Copyright © 2004–2008 Nortel Networks

- **Reset**—if this option is selected, a prompt appears to reset the WLAN IP Telephony Manager 2245 when you exit the SVP-II Configuration screen.
- **Reset all SVP servers**—if this option is selected, all WLAN IP Telephony Manager 2245 units on the subnet are reset.

ATTENTION
Resetting the WLAN IP Telephony Manager 2245 terminates any calls in progress.

Change the password

Nortel recommends that the default password be changed. Follow the steps in Procedure 8 “Changing the password” (page 102) to change the default or existing password.

Procedure 8
Changing the password

Step	Action
1	Select **Change Password** from the **NetLink SVP-II System** menu. The **Change Password** screen appears.
2	Enter the old password, enter the new password, and confirm the new password. The password parameters are as follows: • must be more than four characters in length • first character must be a letter • other characters can be a letter or a number • dashes, spaces, and punctuation marks are not allowed (alphanumeric only)
3	Select **Set Password** and press **Enter**. Alternatively, press the S key on the keyboard. Record the password and keep it in a safe place.

--End--

If you forget the password, use the steps in Procedure 9 “Changing a forgotten password” (page 102) to log on to the SVP server.

Procedure 9
Changing a forgotten password

Copyright © 2004–2008 Nortel Networks

Step	Action
1	Connect your terminal to the RS-232 port using a null-modem cable.
2	To communicate with the gateway, open a terminal emulation program, such as HyperTerminal.
3	Power cycle the SVP server.
4	After the log on prompt appears, within 60 seconds, enter the log on: **maint**
5	At the slnk > prompt, enter the password: **admin** A confirmation message appears to inform you that the password is changed to admin.
6	After the slnk > prompt reappears, enter: **exit**
	--End--

Proceed to configure the wireless handsets. For more information, see *WLAN Handsets Fundamentals (NN43001-505)*, .

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

Administration and maintenance

This section contains information about the following topics:

- “Adding a WLAN IP Telephony Manager 2245 to the system” (page 105)
- “Removing a WLAN IP Telephony Manager 2245 from the system” (page 106)
- “View software version” (page 106)
- “Software updates” (page 107)
- “Wireless handset download messages” (page 110)

Adding a WLAN IP Telephony Manager 2245 to the system

When a WLAN IP Telephony Manager 2245 is added to the system, the change is seamless and does not affect wireless handset calling ability.

A new WLAN IP Telephony Manager 2245 is detected within two seconds of being added to the system (booted, configured, and connected). When detected, any wireless handset not on an active call is immediately forced to check out and check in again. Any wireless handset in a call immediately switches to the WLAN IP Telephony Manager 2245 assigned to provide its timing function. This switchover is not usually noticeable to the user because it is similar to a normal handoff between APs. When the wireless handset ends the call, it is forced to check out and check in again.

Checking in to the Gateway

When a wireless handset is checking in with the WLAN IP Telephony Manager that is providing the Gateway function (not necessarily the same WLAN IP Telephony Manager 2245 that is providing the timing function), the wireless handset is assigned its Alias IP address. Subsequently when the wireless handset checks in with the LTPS, the wireless handset identifies itself with its new Alias IP address to the Call Server. If the wireless handset is checking in again and again, it can indicate a problem on the network, such as poor AP coverage for a user who is moving about. This information is useful when troubleshooting.

Copyright © 2004–2008 Nortel Networks

Removing a WLAN IP Telephony Manager 2245 from the system

When a WLAN IP Telephony Manager 2245 is removed from the system, wireless handsets using the WLAN IP Telephony Manager 2245 are affected. If the removal of the WLAN IP Telephony Manager 2245 is intentional, lock and idle it before removing the WLAN IP Telephony Manager 2245.

When a WLAN IP Telephony Manager 2245 is removed from the system, the removal is detected within two seconds. Wireless handsets not in calls are immediately forced to check out and check in again.

Wireless handset scenarios

For wireless handsets on active calls, two possible scenarios can occur:

- If the removed WLAN IP Telephony Manager 2245 provided the gateway function for the wireless handset, the call is lost and the wireless handset is forced to check in again.
- If the removed WLAN IP Telephony Manager 2245 provided the timing function for the call, the call switches to another WLAN IP Telephony Manager 2245 to provide the timing function.

ATTENTION
During the two seconds while the loss of the WLAN IP Telephony Manager 2245 is being detected, the audio for the call is lost.

View software version

The following sections describe how to view the software version of the hardware.

For the WLAN IP Telephony Manager 2245

To view the software versions for the WLAN IP Telephony Manager 2245, follow the steps in Procedure 10 “Viewing the software version” (page 106).

Procedure 10
Viewing the software version

Step	Action
1	From the WLAN IP Telephony Manager 2245 **NetLink SVP-II System** screen, select **System Status** and press **Enter**.
2	On the **System Status Menu** screen, scroll down to **Software Versions** and press **Enter**. The Software Version Numbers screen displays the software version for each WLAN system component.

Copyright © 2004–2008 Nortel Networks

Ensure that the Functional Code version matches the latest version available from Nortel:

www.nortel.com/support

--End--

For the WLAN Application Gateway 2246

For information about viewing the software versions for the optional WLAN Application Gateway 2246, see Appendix A "Software versions" (page 160).

For a wireless handset

To display the software versions running on a wireless handset, power on the wireless handset and hold down the **Power On/Start Call** key

For the WLAN Handset 6120/6140, Firmware Version is also an option on the Config menu.

Software updates

Nortel provides information about software updates. Download the software updates. You must download the file of Product Category: Wireless LAN, Product Name: Wireless Telephony Manager 2245, Content type: Releases. Obtain the precise Release, Status, and Title of the file from your next level of support. See www.nortel.com/downloadingcontent.

After obtaining the software updates from Nortel, transfer them to the TFTP Server accessed by the WLAN IP Telephony Manager 2245.

Update software on the WLAN IP Telephony Manager 2245

To update the software on the WLAN IP Telephony Manager 2245, reset it. When the WLAN IP Telephony Manager 2245 starts up, it compares its software version to the software version on the TFTP Server. The WLAN IP Telephony Manager 2245 downloads the software from the TFTP Server if the versions are different.

CAUTION

Always ensure that only the latest version of software is on the TFTP Server and that earlier software versions are deleted, moved, or renamed.

At startup, the WLAN IP Telephony Manager 2245 always uses TFTP, if configured in the 2245, to compare its software version with the version on the TFTP Server. If the versions are different, the WLAN IP Telephony Manager 2245 downloads the software version from the TFTP Server, even if it is an older version.

Copyright © 2004–2008 Nortel Networks

Lock the system

Always lock the WLAN IP Telephony Manager 2245 in the SVP-II Configuration screen before updating the software. Locking the WLAN IP Telephony Manager 2245 prevents new calls from starting.

Reset the WLAN IP Telephony Manager 2245 after the update is complete.

ATTENTION
All calls in progress are terminated when the WLAN IP Telephony Manager 2245 is reset.

Update software on the WLAN Application Gateway 2246

For information about updating the software on the optional WLAN Application Gateway 2246, see Appendix A "Software" (page 161).

Update software on a wireless handset

With the WLAN system, you can perform over-the-air transfer of software updates from the designated TFTP Server to the wireless handsets.

The downloader function in the wireless handset checks its software version every time the wireless handset is turned on. If there is any difference in the software version, the wireless handset immediately begins to download the update.

On a clear 802.11a/b/g channel, the download process takes one minute or less to complete.

If the TFTP Server cannot be reached at the time the wireless handset is powered on, resets, or comes back into a WLAN service area, the wireless handset tries a few times to contact the TFTP Server, and then gives up and uses the existing software.

If more wireless handsets are requesting TFTP service than the TFTP Server has ports available, or if the TFTP Server is unreachable or unavailable, the wireless handsets try a few times to reach the TFTP Server, and then continues to use the existing software. In other words, it is not possible to guarantee that a wireless handset is using the latest software.

For example, it is not possible to guarantee that all wireless handsets are upgraded as a result of an isetResetAll command. To verify that a wireless handset is running the intended version of software, use the isetShow command to determine the software version.

Copyright © 2004–2008 Nortel Networks

From the Signaling Server or Voice Gateway Media Card, use the oam> or IPL> isetGet command to display a list of all currently registered wireless handsets that are running the old firmware version. Use this command on all LTPS Signaling Servers or Voice Gateway Media Cards that have IP Phones and wireless handsets currently registered:

oam> isetGet fwvsn==<old 221022112212 firmware version>

Software update (version 97.071) for the WLAN Handsets 2210/2211/2212

To download version 97.071 of the software for the WLAN Handsets 2210/2211/ 2212, follow Procedure 11 “Updating software for the WLAN Handsets 2210/ 2211/ 2212” (page 109). Version 97.070 is compatible with new or existing wireless handsets.

Procedure 11
Updating software for the WLAN Handsets 2210/ 2211/ 2212

Step	Action
1	Go to www.nortel.com.
2	Follow the instructions at www.nortel.com/downloadingcontent to download the following file: • Product Category: Wireless LAN, , • Product Name: Wireless Telephony Manager 2245 • Content type: Releases. Obtain the precise Release, Status, and Title of the file from your next level of support.
3	Select **Find Products > A-Z**.
4	Select **W**.
5	Scroll to **WLAN Handset 2210/2211/2212** and select **Software**.
6	Select **WLAN – Handsets 2210/2211 Firmware version 97.070**.

--End--

For more information, see *WLAN Handsets Fundamentals (NN43001-505)*, .

Displays

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions, and downloading the software. During the download, a progress bar on the wireless handset display screen displays the progress of the download.

Copyright © 2004–2008 Nortel Networks

ATTENTION
IMPORTANT!
While the wireless handset is updating the software, the NO SVC message displays, and the wireless handset must not be powered off. For approximately 10 seconds, the wireless handset cannot be powered off. A warning message appears during that time. If the warning message is not displayed, the wireless handset can be powered off without damage.

When the update is complete, the wireless handset displays the extension number, and is ready for use.

Wireless handset download messages

Normal download messages

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the software versions, and downloading. The normal message progression is listed in Table 13 "Normal download messages" (page 110)

Table 13
Normal download messages

Message	Description
Checking Code	Wireless handset is contacting the TFTP Server to determine if the server has a newer version of software that must be downloaded.
Erasing Memory	Wireless handset has determined that a download must occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line, the erase operation is complete.
Updating Code	Wireless handset is downloading new software into memory. This message also displays a progress bar. When the progress bar fills the display line, the update operation is complete on that file.

When the update is complete, the wireless handset displays the extension number, and is ready for use.

Download failure or recovery messages

Table 14 "Failure and recovery messages" (page 110) lists the display messages for the wireless handset that indicate a failure or recovery situation during the software download process.

Table 14
Failure and recovery messages

Message	Description
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other handsets and refusing additional downloads. The wireless handset automatically retries the download every few seconds.

Copyright © 2004–2008 Nortel Networks

Table 14
Failure and recovery messages (cont'd.)

Message	Description
TFTP Error (x):yy	A failure occurred during the TFTP download of one of the files. **(x)** = the file number that was being downloaded. **yy** = an error code describing the particular failure. Possible error codes are: • 01 = TFTP Server did not find the requested file. • 02 = Access violation (reported from TFTP Server). • 07 = TFTP Server reported No such user error. Check the TFTP Server configuration. • 81 = File put into memory did not CRC. The wireless handset attempts to download the file again. • FF = Timeout error. TFTP Server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the wireless handset. This operation retries.
Waiting	Wireless handset has attempted an operation several times and failed, and is now waiting for a period of time before attempting that operation again.
Internal Error OE	OE = Error while writing the Flash (return wireless handset to Nortel).

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

Troubleshooting

This chapter contains information about the following topics:

- “Troubleshooting the WLAN IP Telephony Manager 2245” (page 113)
- “Troubleshooting the WLAN Application Gateway 2246” (page 116)
- “Troubleshooting the handset” (page 116)
- “Dropped calls” (page 119)
- “Troubleshooting coverage issues” (page 139)
- “Before calling Nortel Technical Support” (page 139)

Troubleshooting the WLAN IP Telephony Manager 2245

Use the System Status Menu screen to obtain information about system alarms and network status.

For information about how to connect to the WLAN IP Telephony Manager 2245 and access the System Status Menu screen from the NetLink SVP-II System screen, see “WLAN IP Telephony Manager 2245 configuration” (page 93).

Options on the System Status Menu screen provide a window into the real-time operation of the system components. Use this data to evaluate system function and to troubleshoot areas that can be experiencing problems.

On the System Status Menu screen, select from the following options:

- **Error Status**—displays alarm and error message information.
- **Network Status**—displays information about the Ethernet network to which the WLAN IP Telephony Manager 2245 is connected.
- **Software Versions**—lists the software versions for the WLAN IP Telephony Manager 2245.

Copyright © 2004–2008 Nortel Networks

Error Status screen

The Error Status screen displays any alarms that indicate some system malfunction. Some of these alarms are easily remedied. Others require a call to Nortel Technical Support.

From the System Status Menu screen, select Error Status. The Error Status screen displays active alarms on the WLAN IP Telephony Manager 2245. Table 15 "WLAN IP Telephony Manager 2245 active alarms and actions" (page 114) lists the alarms and the actions required to eliminate the alarm.

Table 15
WLAN IP Telephony Manager 2245 active alarms and actions

Alarm text	Action
Maximum payload usage reached	Reduce usage, clear alarm
Maximum telephone usage reached	Reduce usage, clear alarm
Maximum Access Point usage reached	Reduce usage, clear alarm
Maximum call usage reached	Reduce usage, clear alarm
SRP audio delayed	Reduce usage, clear alarm
SRP audio lost	Reduce usage, clear alarm
No IP address	Configure an IP address

Press **C** to clear all clearable alarms.

Network Status screen

The WLAN IP Telephony Manager 2245 is connected to the Ethernet network (LAN). The information about that connection is provided on the Network Status screen. The screen displays information about the Ethernet network. This information can help troubleshoot network problems.

To access the Network Status screen, select Network Status from the System Status Menu screen.

Use the Network Status screen to view the following information:

- **Ethernet Address**—media access control (MAC) address of the WLAN IP Telephony Manager 2245 (hexadecimal).
- **System Uptime**—the number of days, hours, and minutes since the WLAN IP Telephony Manager 2245 was last reset.
- **Net**—the type of connection to the Ethernet switch currently utilized. Displayed as 10 (10BaseT) or 100 (100BaseT) half-duplex, or full-duplex.

Copyright © 2004–2008 Nortel Networks

- **Max (maximum) calls**—number of calls that can be supported by the WLAN IP Telephony Manager 2245 (depends on network speed).
- **RX**—Ethernet statistics about the received signal during System Uptime.
  - **bytes**—number of bytes received
  - **packets**—number of packets received
  - **errors**—sum of all receive errors (long packet, short packet, CRC, overrun, alignment)
  - **drop**—packets dropped due to insufficient memory
  - **fifo**—overrun occurred during reception
  - **alignment**—non-octet-aligned packets (number of bits not divisible by 8)
  - **multicast**—packets received with a broadcast or multicast destination address
- **TX**—Ethernet statistics about the transmitted signal during System Uptime.
  - **bytes**—number of bytes transmitted
  - **packets**—number of packets transmitted
  - **errors**—sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier)
  - **drop**—packets dropped due to insufficient memory
  - **fifo**—underrun occurred during transmission
  - **carrier**—count of carrier losses during transmission
  - **collisions**—packets deferred (delayed) due to collision
- **SVP-II Access Points in Use**—number of APs in use by wireless handsets, either in standby or in a call. **Last** is current use, **Max** is the maximum number in use at one time.
- **SVP-II Access Points in Calls**—number of APs with wireless handsets in a call.
- **SVP-II Telephones in Use**—number of wireless handsets in standby or in a call.
- **SVP-II Telephones in Calls**—number of wireless handsets in a call.
- **SVP-II SRP Audio (Delay)**—SRP audio packets whose transmission is momentarily delayed
- **SVP-II SRP Audio (Lost)**—SRP audio packets dropped due to insufficient memory resources

Copyright © 2004–2008 Nortel Networks

Software Version Numbers screen

The Software Version Numbers screen provides information about the software version currently running on the WLAN IP Telephony Manager 2245.

This information helps to determine if the most recent software version is running. This information assists Nortel Technical Support in troubleshooting software problems.

Speed or duplex mismatch

A duplex mismatch on the WLAN can cause the WLAN IP Telephony Manager 2245 to not operate properly. Double-check WLAN connections and interfaces to ensure that they are all configured as full-duplex.

In rare instances, the message Speed or Duplex mismatch error can occur during the bootup sequence of the IP Telephony Manager 2245.

If this situation occurs, verify all devices connected to the WLAN IP Telephony Manager 2245 are configured correctly and no duplex mismatch is found. If all configurations are correct, reboot the IP Telephony Manager 2245. The error message must be cleared.

Nortel recommends that you

- do not configure the Ethenet Link, on the SVP-II Configuration screen, to auto-negotiate.
- use either 100/full or 10/full, as is appropriate for the network.
- configure the ethernet switch port to match the 2245 Ethernet Link.

Troubleshooting the WLAN Application Gateway 2246

For information about troubleshooting the optional WLAN Application Gateway 2246, see “WLAN Application Gateway 2246” (page 141) “Configuring network parameters” (page 149).

Troubleshooting the handset

Transmission problems can result from any number of factors originating from the wireless LAN. Wireless handsets can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting wireless handsets, consider the following problem sources to determine the best method of approaching a specific situation.

Copyright © 2004–2008 Nortel Networks

Context

When troubleshooting a problem with a wireless handset, it is important to determine the context of when and where the problem occurred. Context includes the following:

- Was the wireless handset on an active call?
- Was the wireless handset moving or stationary?
- Was the wireless handset powering on or powering off?
- Was PTT being used?
- At what location did the problem occur?

Record this information and provide it to the system administrator or Nortel Technical Support.

Access Point problems

Most, but not all, wireless handset audio problems are related to AP range, positioning, and capacity. Performing a Site Survey as described in "Site survey" (page 33) can isolate the AP causing these types of problems. If the wireless handset itself is suspected, conduct a parallel site survey with a wireless handset that is known to be functioning properly.

The following are some situations that can cause wireless handset difficulties to occur:

- **In range/Out of range**—service is disrupted if a user moves outside the area covered by the WLAN APs. Service is restored if the user moves back within range. If a call drops because a user moves out of range, the wireless handset recovers the call if the user moves back into range within a few seconds.
- **Capacity**—in areas of heavy use, the call capacity of a particular AP can be filled. If this happens, the user hears three chirps from the wireless handset. The user can wait until another user terminates a call, or move within range of another AP and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another AP. Due to range limitations, this can be the same as moving out of range.
- **Transmission Obstructions**—before system and AP installation, the best location for APs for optimum transmission coverage is determined when a site survey is performed. However, small pockets of obstruction can still be present, or obstructions can be introduced into the facility after AP installation. This loss of service can be restored by moving out of the obstructed area, or by adding more APs.

Copyright © 2004–2008 Nortel Networks

Configuration problems

Certain problems are associated with improper configuration of either the WLAN IP Telephony 2245, the optional WLAN Application Gateway 2246, or the wireless handset.

Configuration problems are generally corrected by changing the configuration on the WLAN IP Telephony 2245, the WLAN Application Gateway 2246, or the wireless handset.

There can also be incorrect programming of the APs. For compatibility and configuration information about the APs in use at the site, see “Compatible Access Points” (page 215).

Duplex mismatch

A duplex mismatch on the WLAN can cause the wireless handsets to not operate properly. Double-check WLAN connections and interfaces to ensure that they are all configured as full-duplex.

No ring

It is possible in certain situations for a voice mail message to be left on a wireless handset without the wireless handset ever ringing. This situation could occur when a wireless handset is out of range of an AP for even a few seconds. If during the time the wireless handset is out of AP range and an incoming call is received, the incoming call receives the Call Forward No Answer (CFNA) treatment configured for that wireless handset, such as forwarding the incoming call to voice mail.

To prevent this situation from occurring, ensure adequate AP coverage in all areas where a wireless handset is used.

Far-end echo

Sometimes, when using the G.711 codec, echo might be perceptible at the far end, and be more severe when the wireless handset is in an environment with extreme background noise and the wireless handset volume is set to maximum volume.

To correct this problem, reduce the volume setting on the wireless handset, , the microphone gain or both.

You can change the microphone gain from the Standby Menu, Noise Mode.

Alternatively, if you experience this problem, consider using the G.729 codec.

Copyright © 2004–2008 Nortel Networks

Dropped calls

If calls are dropping, use the Site Survey mode of the wireless handset in the area where the problem occurred to determine if there is inadequate AP coverage in that area.

Wireless handset status messages

Wireless handset status messages provide information about the handset communication with the AP and Call Server. Table 16 "Wireless handset status messages" (page 119) summarizes the status messages, in alphabetical order.

Table 16
Wireless handset status messages

Message	Description	Action
3 chirps	Wireless handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning. The call is handed-off to the best AP after it becomes available.
Address Mismatch	Wireless handset software download files are incorrect or corrupted.	Download new software from the Nortel site. See “Software updates” (page 107).
ASSERT xxx.c Line yyy (For WLAN Handsets 2210/2211/2212 only.)	The handset has detected a fault from which it cannot recover.	Record the error information so that it can be reported. Turn the handset off, and then on again. If the error persists, try registering a different handset to this telephone port. If the error still persists, contact Nortel Technical Support and report the error.
Assoc Failed xxxxxxxxxxxx	x...x = AP MAC address Handset association is refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per the Configuration Note. Try another AP.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Assoc Timeout xxxxxxxxxxxx	x...x = AP MAC address Handset did not receive an association response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per the Configuration Note. Try another AP.
Auth Failed xxxxxxxxxxxx	x...x = AP MAC address Handset authentication is refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per the Configuration Note. Try another AP.
Auth Timeout xxxxxxxxxxxx	x...x = AP MAC address Handset did not receive an authentication response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per the Configuration Note. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software license types Handset software does not match the current handset license selection.	Download new software from the Nortel site. See "Software updates" (page 107).
Bad Config	Some needed configuration parameter has not been set.	Check all required wireless handset configuration parameters for valid settings.
Bad ESSID (For WLAN Handsets 2210/2211/2212 only.)	The wireless handset is configured for static ESSID (as opposed to Learn once or Learn always) and no ESSID is entered.	Enter an ESSID in the configuration settings or change to one of the Learn modes.
Bad SSID (For WLAN Handsets 6120/6140 only.)	The wireless handset is configured for static SSID (as opposed to Learn once or Learn always) and no SSID is entered.	Enter an SSID in the configuration settings or change to one of the Learn modes.
Bad Local ID	The value of the Phase 1 Local ID type entered in the handset through the menus or the Configuration Cradle is improperly configured.	Enter a valid ID value.
Bad Local ID Type	The Phase 1 Local ID type entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid ID type. KEY ID is the only valid choice.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Bad Network IP	The value of the Remote Network IP address entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid remote network IP address.
Bad Network Mask	The value of the network mask for the Remote Network entered in the handset through the menus or the Configuration Cradle is missing or invalid.	Enter a valid network mask.
Bad Payload Type	The VPN server is not accepting some of the parameters passed to it by the handset. One common instance is if two handsets try to use the Client IP.	If the VPN Client IP is statically configured, ensure that the address assigned to the handset is unique. If using IKE Mode Config, ensure that the address entered in the VPN Server configuration for the handset or user is unique.
Bad Phintl File	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site. See "Software updates" (page 107).
Bad Program File	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site. See "Software updates" (page 107).
Bad Preshared Key	The value of the preshared key entered in the handset through the menus or Configuration Cradle is improperly configured.	Enter a valid preshared key value. For a Contivity VPN server, this is the password.
Bad Tunneled IP	The value of the VPN Client IP address entered in the handset through the menus or the Configuration Cradle is configured for static IP and is missing.	Enter a valid client IP address.
Bad VPN Server IP	The VPN Server IP address entered in the handset through the menus or the Configuration Cradle is invalid.	Enter the IP address of the VPN server.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
(battery icon), Low Battery message, and beep Battery Low	Low battery	**In call**: the battery icon displays and a soft beep is heard when the user is on the wireless handset and the battery charge is low. User has approximately 15 to 30 minutes of battery life left.
Battery Low		The **Battery Low** message indicates that the battery pack can be changed while the call is still in progress. For the WLAN Handsets 2210/ 2211/2212 only, do not press **Power Off/End Call**. Place the call on Hold or Park, quickly remove the discharged battery and replace with a charged battery, power on the handset and press **Power On/Start Call** to resume the call in progress. For the WLAN Handsets 6120/ 6140 only, do not press End. Place the call on Hold or Park, quickly remove the discharged battery and replace with a charged battery, power on the handset and press Start to resume the call in progress. **Not in call**: The battery icon displays whenever the battery charge is low. The message **Low Battery** and a beep indicate a critically low battery charge when user is not on the wireless handset. The wireless handset does not work until the battery pack is charged.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Battery Failure	The battery pack is not functioning.	Replace the battery pack with a new or confirmed battery pack. Only the approved battery pack works.
Battery Failed	Battery pack is damaged or incompatible with the handset.	Replace the battery pack with a new or confirmed battery pack. Only the approved battery pack works.
Can't renew DHCP yyy.yyy.yyy.yyy	y...y = DHCP server IP address DHCP server is not responding to the initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.
Charging ...	The wireless handset is charging in the Desktop Charger.	No action needed.
Charge Complete	The wireless handset is now fully charged.	No action needed.
Checking Code	Wireless handset is contacting the TFTP Server to determine if it has a newer version of software that must be downloaded.	None. This message usually only lasts for approximately one second. If message remains displayed, power off and contact Nortel Technical Support.
Checking DHCP IP	The wireless handset is retrieving DHCP information from the DHCP server.	None. This is for information only.
CRC Code Error	The software that is TFTP downloaded has a bad Cyclical Redundancy Code (CRC) check.	Try the download again. It is possible the software became corrupted during download. If the error repeats, check that the download image on the TFTP Server is not corrupted.
Code Mismatch!	The software loaded into the wireless handset is incorrect for this model of telephone.	Verify that the License Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.
DCA Timeout	The handset has detected a fault from which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, and then on again. If the error persists, contact Nortel Technical Support and report the error.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
DHCP Error (1-5)	DHCP Error 1	The wireless handset cannot locate a DHCP server. It tries every 4 seconds until a server is located.
	DHCP Error 2	The wireless handset has not received a response from the DHCP server to a request for an IP address. It retries until a DHCP server is found.
	DHCP Error 3	The server refuses to lease the wireless handset an IP address. It keeps trying.
	DHCP Error 4	The DHCP server offered the wireless handset a lease that is too short. The minimum lease time is 10 minutes. One hour is the minimum recommended lease time. The wireless handset stops trying. Reconfigure the DHCP server and power-cycle the wireless handset.
	DHCP Error 5	Failure during WEP Key rotation process (proprietary failure).
DHCP Lease Exp yyy.yyy.yyy.yyy	y...y = DHCP Server IP address DHCP is not responding to renewal attempts. At least one renewal succeeded.	The wireless handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration is changed by the administrator. The wireless handset attempts to negotiate a new lease or display one of the DHCP errors (1-5).
DHCP NACK error yyy.yyy.yyy.yyy	y...y = DHCP Server IP address DHCP server explicitly refused renewal.	The DHCP lease currently in use by the wireless handset is no longer valid, which forces the wireless handset to restart. This problem resolves itself on the restart. If it does not, the problem is in the DHCP server.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
DL Not On Sector	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site. See "Software updates" (page 107).
DO NOT POWER OFF	The wireless handset is in a critical section of the software update.	None. Do not remove the battery or attempt to power off the phone while this message is displayed. Doing so can require the wireless handset to be returned to Nortel to be recovered.
Duplicate IP	The wireless handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the wireless handset is assigned a unique address.
Erase Failed	Download process failed to erase the memory in the wireless handset.	Operation retries but can eventually report the error int. error: 0F. Power cycle the wireless handset.
Erasing memory	The wireless handset has determined that a download must occur and is erasing the current software from memory.	None. When the progress bar fills the display line, the erase operation is complete. Do not turn the handset off during this operation.
Error! [error details] (For the WLAN Handset 6120/6140 only)	A fatal software error is detected. All handset operation is halted and any call is lost.	This message appears during the Halt on Error mode. To capture the error message, reboot the handset and write down the information that is on the display.
Files Too Big	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site. See "Software updates" (page 107).

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Flash Config Error	Handset internal configuration is corrupt.	Perform the Restore Defaults operation from the administrator menu and reprogram, or reprogram using the Configuration Cradle.
Initializing	The wireless handset is performing a power-on initialization.	None. This is informational only.
Internal Err. # #	The wireless handset has detected a fault from which it cannot recover. OE=Error while writing the Flash (return handset to factory) OF = No functional code (contact Nortel Technical Support)	Record the error code so it can be reported. Turn the wireless handset off, and then on again. If the error persists, try registering a different wireless handset to this telephone port. If the error still persists, contact Nortel Technical Support and report the error.
Invalid ID Info	The VPN server did not recognize this user.	Make sure that the local ID (KEY ID) entered in the handset matches the key ID in the VPN server. For a Contivity VPN server, the local ID must match the username.
Multiple SVP Svr yyy.yyy.yyy.yyy	y...y = WLAN IP Telephony Manager 2245 IP address Handset received responses from multiple WLAN IP Telephony Manager 2245 units; displays the IP address of one responding WLAN IP Telephony Manager 2245.	Happens if the handset is reconfigured to use a different WLAN IP Telephony Manager 2245 and then powered-down before the previous server has had time to determine that the handset is no longer connected to it. The problem usually corrects itself in about 30 seconds.
Must upgrade SW!	Handset software is incompatible with the hardware.	Download new software from the Nortel site. See "Software updates" (page 107).
Net Busy xxxxxxxxxxxx	x...x = AP MAC address Handset cannot obtain sufficient bandwidth to support a call; displays the MAC of the failing AP.	Try call again later.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to the WLAN or use Static IP configuration in the handset.
No ESSID (For the WLAN Handsets 2210/2211/ 2212 only.)	Attempted to run the site survey application without an ESSID configured.	Let the handset come completely up. Statically configure an ESSID in the Admin menu.
No SSID (For the WLAN Handsets 6120/6140 only.)	Attempted to run the site survey application without an SSID configured.	Let the handset come completely up. Statically configure an SSID in the Admin menu.
No Func Code	Handset software download files are incorrect or corrupt.	Reconfigured the handset to gain access to the WLAN and download new code.
No Host IP (Addr)	The wireless handset is configured for static IP (as opposed to use DHCP) and no valid host IP address (the wireless handset IP address) is entered.	Enter a valid IP address in the configuration settings or change to use DHCP.
No IP Address	Invalid IP address.	Check the IP address of the wireless handset and reconfigure if required.
No Net Access	Cannot authenticate or associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found (For the WLAN Handsets 2210/2211/ 2212 only.)	This indicates any of the following:	
	• No radio link	Verify that the AP is turned on.
	• No ESSID—Autolearn not supported (or) incorrect ESSID	Verify the ESSID of the wireless LAN and enter or Autolearn it again, if required.
	• AP does not support appropriate data ranges	Check the AP configuration against the AP Configuration Note.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
	• Out of Range	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of the handset.
	• Incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	• Incorrect Security settings	Verify that all the Security setting in the AP.
No Net Found (For the WLAN Handsets 6120/6140 only.)	This indicates any of the following:	
	• No radio link	Verify that the AP is turned on.
	• No ESSID—Autolearn not supported (or) incorrect SSID	Verify the SSID of the wireless LAN and enter or Autolearn it again, if required.
	• AP does not support appropriate data ranges	Check the AP configuration against the AP Configuration Note.
	• Out of Range	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the SSID of the handset.
	• incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	• Incorrect Security settings	Verify that all the Security setting in the AP.
No Net Found xxxxxxxxxxxx yy	x...x = AP MAC address yy = AP signal strength Handset cannot find a suitable AP; displays the MAC address and signal strength of the best nonsuitable AP found.	Check the AP and handset network settings, such as ESSID, (for the WLAN Handsets 2210/ 2211/2212), SSID (for WLAN Handsets 6120/6140), Security, Reg. domain and Tx power. Ensure that the APs are configured per the Configuration Note. Try Site Survey mode to

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
		determine a more specific cause.
No PBX Response	The wireless handset tried to send a message to the Call Server and failed to get a response.	Verify the Call Server is operational and connected to the network.
No Proposal	The handset and the VPN server cannot agree on a set of configuration parameters.	Check that the Diffie-Hellman group, phase 1 and phase 2 hashes, and the encryption algorithms configured on the handset are acceptable to the VPN server.
No Reg Domain	Regulatory Domain not set	Configure the Regulatory Domain of the handset.
No SVP IP	The wireless handset is configured for static IP (as opposed to use DHCP) and no valid WLAN IP Telephony Manager 2245 address is entered.	Enter a valid WLAN IP Telephony Manager 2245 IP address in the wireless handset configuration setting or change to use DHCP.
No SVP Response yyy.yyy.yyy.yyy	y...y = SVP Server IP address The handset has lost contact with the WLAN IP Telephony Manager 2245.	This can be caused by bad radio reception or a problem with the WLAN IP Telephony Manager 2245. The handset keeps trying to fix the problem for 20 seconds, and the message can clear by itself. If it does not, the handset restarts. Report this problem to the system administrator if it keeps happening.
No SVP Server	Wireless handset cannot locate WLAN IP Telephony Manager 2245.	IP address configuration of WLAN IP Telephony Manager 2245 is wrong or missing.
	WLAN IP Telephony Manager 2245 is not working.	Check error status screen on WLAN IP Telephony Manager 2245.
	No LAN connection at the WLAN IP Telephony Manager 2245.	Verify WLAN IP Telephony Manager 2245 connection to LAN.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
No SVP Server No DNS Entry	The handset is unable to perform DNS lookup for the WLAN IP Telephony Manager 2245; server had no entry for SVP Server.	The network administrator must verify that a proper IP address is entered for the SVP Server DHCP option.
No SVP Server No DNS IP	The handset is unable to perform a DNS lookup for the WLAN IP Telephony Manager 2245; no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been properly identified.	Check that the handset license type has a corresponding entry in the slink_cfg.cfg file. Check that the pd11ccc.bin and pi110003.bin entries exist under this type in the slnk_cfg.cfg.
No UNIStim DHCP	The handset is unable to use DHCP to obtain the server information it requires to start up.	Verify the DHCP server configuration information. Verify network connectivity between the handset and the DHCP server.
No VPN Server	The handset cannot find the VPN server.	Check that the value of the VPN Server IP address configured through the administration menu or the Configuration Cradle match the address of the VPN server.
Not Installed!	A required software component is missing.	Check that all required software files are on the TFTP Server, if over-the-air downloading is being used. If the error repeats, contact Nortel Technical Support.
Payload Malfmd	The handset cannot understand an encrypted message from the VPN Server (or vice-versa). This is likely to be a mismatch in the security parameters such as preshared key, Diffie-Hellman group, hash and encryption algorithms.	Check the Diffie-Hellman group, the phase 1 and phase 2 hashes, and encryption configuration.
Press End Call	The call has ended.	Press the Power Off/End Call key to return to standby mode.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Restart Command	The wireless handset received a restart command from the Call Server.	None. The wireless handset automatically restarts in a few seconds.
RTP Open Failed	The handset is unable to open the requested RTP or RTCP socket.	Reboot the handset. If the error repeats, contact Nortel Technical Support.
Select License	The correct protocol has not been selected from the license set.	Using the administrative menus, select one license from the license set to allow the wireless handset to download the appropriate software.
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other devices and refusing additional downloads.	None. The wireless handset automatically retries the download every few seconds.
Server Unavailable. Restarting... (For the WLAN Handset 6120/6140 only)	An error caused the handset to lose the call. It is trying to restart and return to standby mode.	Occurs during Restart on Error mode. The handset is attempting to register with the PBX and resume normal operation. Error details may be available through the Syslog Server and by download with the Handset Administration Tool.
SKT Open Failed	Socket open fail. Occurs when the handset tries to connect to the call server, but there is no response. If resiliency is active, the handset keeps trying.	If the call server is inoperative and resiliency is not active, or the handset cannot locate a backup call server, turn off the handset and repair the primary call server. Nortel recommends that you reconfigure the backup call server to be the primary call server if the repair is more time-consuming than the reconfiguration.
Storing Config	Handset is storing changes to handset configuration.	None. Informational message only. The handset can display this briefly following a configuration change or software download.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
SVP Service Rej.	The WLAN IP Telephony Manager 2245 has rejected a request from the wireless handset.	The wireless handset restarts and attempts to reregister with the WLAN IP Telephony Manager 2245, which usually fixes the problem. Report this to the administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy (with busy tone)	y...y = SVP or GW IP Address Gateway or WLAN IP Telephony Manager has reached call capacity; displays the IP address of the gateway SVP Server.	All call paths are in use; try call again in a few minutes.
System Locked (with busy tone)	WLAN IP Telephony Manager 2245 is locked. Gateway is locked.	Try call again later. System is locked for maintenance.
TFTP ERROR(x):yy	A failure occurred during a TFTP software download. **(x)** = the file number that was being downloaded; **yy** = an error code describing the particular failure. Possible error codes are: • 01 = TFTP Server did not find the requested file. • 02 = Access violation (reported from TFTP Server). • 07 = TFTP Server reported No such user error. • 81 = File put into memory did not CRC. • FF = Timeout error. TFTP Server did not respond within a specified period of time.	Error code 01, 02 or 07—check the TFTP Server configuration. Error code 81—the wireless handset attempts to download the file again. For other messages, power off the wireless handset, and then turn it on again to retry the download. If the error repeats, note it and contact Nortel Technical Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Nortel.

Copyright © 2004–2008 Nortel Networks

Table 16
Wireless handset status messages (cont'd.)

Message	Description	Action
Unknown xx:yy:zz	A phrase is missing from your phintl file.	Download new software from the Nortel site. See "Software updates" (page 107).
Updating Code	Wireless handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line, the update operation is complete on that file.	None. When the progress bar fills the display line, the update operation is complete on that file. Do not turn off the handset during this operation.
VPN Error: xxxx	The VPN server returned an information message with a code of xxx.	
Waiting	Wireless handset has attempted some operation several times and failed. It is now waiting for a period of time before attempting that operation again.	None. The wireless handset is waiting for a specified period of time before attempting that operation again.
Watchdog Timeout	The wireless handset failed to hear from the Call Server within the watchdog timeout interval.	Verify the Call Server is operational and connected to the network.
Wrong Code Type	The software loaded into the handset is incorrect for this model of handset.	Verify that the license type is set correctly. If the license type is correct, replace the software image on the TFTP server with the software that is correct for the handset model.

Using Call Server overlay commands

The following sections provide information about Call Server overlay commands.

Copyright © 2004–2008 Nortel Networks

LD 32 IDU command

For the handsets, the IDU command outputs the following specific information:

- Release code: Rls: 6 (2210), Rls: 7 (2211) or Rls: 8 (2212)
- NT Code: NTTQ4010 (2210), NTTQ5010 (2211) or NTTQ69AA (2212)
- Software Version has different format: <Version>.<Issue> FWSW:097.070 (or later)
- The IP address is the alias IP address of the wireless handset that is provided by the WLAN IP Telephony Manager 2245. The MAC address is the MAC address of the wireless handset. In other words, the MAC address and the IP address are not related.

In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211.

```
.idu 61 0
I2004 TN: 061 0 00 00 V
TN ID CODE: i2004
ISET MAC ADR: 00:60:38:76:41:C7
ISET IP ADR: 192 .168 .010 .100
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NT2K00GI
COLOR CODE: 66
RLS CODE: 0
SER NUM: 7641C7
FWSW VERSION: 0602B59
.idu 62 2
I2004 TN: 062 0 00 02 V
TN ID CODE: i2004
ISET MAC ADR: 00:90:7A:01:7E:47
ISET IP ADR: 192 .168 .010 .200
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NTTQ5010
COLOR CODE: 66
RLS CODE: 7
SER NUM: 017E47
FWSW VERSION: 097.021
```


Copyright © 2004–2008 Nortel Networks

LD 32 STAT command

The wireless handsets are shown REGISTERED in the standby and active modes. In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211 in the standby mode.

```
.stat 61 0
IDLE REGISTERED 00
.stat 62 2
IDLE REGISTERED 00
```

LD 117 Inventory command

In the inventory report, the wireless handsets have a specific release code and NT code, similar to the IDU command output. In the following example, 61 0 is an IP Phone 2004 and 62 2 is a WLAN Handset 2211.

```
=> inv prt sets
Set inventory:
17 10 2003 8 17 21, 17 10 2003 8 17 22, 6
i2004, 61 00, i2004 NT2K00GI 66 0 7641C7, I2004 , 6000
i2004, 62 02, i2004 NTTQ5010 66 7 017E47, I2211 , 6502
```

LD 117 STIP command

The STIP command can be used for wireless handsets; however, the wireless handset alias IP address appears as the TERMIP in the command output, instead of physical IP address. In the following example, the 192.168.10.200 is an alias IP address assigned by the WLAN IP Telephony Manager 2245.

```
TN HWID STATUS HOSTIP TERMIP PORT
_____ ____________________________ _____ _____________
____________ _______
0x600a 00000000000003000907a017e476607 REG 47.11.214.165
192.168.10.200 0x1450
CAPS

_________
0x00000000
-------------------------------
codec bdwth(k) codecCaps desc
-------------------------------
4 190 0x00000000 1
3 190 0x00000000 1
17 47 0x00000001 1
value = 537232412 = 0x2005841C
```

For information about more CLI commands, see “Zones” (page 71).

Copyright © 2004–2008 Nortel Networks

TPS CLI commands

The following sections describe TPS command line interface (CLI) commands.

dsetShow command

In the **dsetShow** command output, the handsets have a specific Hardware ID. The alias IP address is output, not the physical wireless handset IP address.

In the following example, the IP Phone 2004 has an IP address of 192.168.10.100 and the WLAN Handset 2211 has an alias IP address of 192.168.10.200. The syntax of the Hardware ID is as follows:

- first two digits—Manufacturer Location. Manufacturer Location is 18 for the IP Phone 2004 and 30 for the WLAN Handset 2211.
- next six digits—Manufacturer Code. The Manufacturer Codes are defined as follows:
  - IP Phone 2004 Phase 1—006038
  - IP Phone 2004 Phase 2—000ae4
  - WLAN Handset 2210—00907a
  - WLAN Handset 2211—00907a
  - WLAN Handset 2212—00907a
- last two digits—Release Code. The Release Codes are defined as follows:
  - IP Phone 2004 Phase 1—0
  - IP Phone 2004 Phase 2—2
  - WLAN Handset 2210—0x06
  - WLAN Handset 2211—0x07
  - WLAN Handset 2212—0x08

```
-> dsetShow
TN IP Address Hardware ID TermType
---- --------------- ------------------ ----------
6004 192.168.10.100 180060387641c76600 i2004
600A 192.168.10.200 3000907a017e476607 i2004
value = 0 = 0x0
```

e2dsetShow command

The **e2dsetShow** command is used for the handsets in the same manner as for the IP Phones.

Copyright © 2004–2008 Nortel Networks

isetCount and isetGet

Use the alias IP address of the handsets in the expression string of the **isetCount** and **isetGet** commands, not the physical IP address. The following is an example of the **isetGet** output for the WLAN Handset 2211.

```
->isetGet "IP == 192.168.10.200"
IP Address Type RegType State Up Time Set-TN Regd-TN HWID
FWVsn
---------- ----- ------- ----- ------- ------- -----
------------ ---------
192.168.10.200 i2004 Regular online 0 00:12:00 062-02
062-02 3000907a017e476607 097.021

UNIStimVsn SrcPort DstPort
--------- ------ ------
2.6 5100 5000
```

isetReset and isetResetAll

The **isetReset** command can be used to reset the wireless handsets by specifying the wireless handset alias IP, not the physical IP address:

```
-> isetReset "192.168.10.200"
value = 0 = 0x0
```

isetShow, isetShowByTN, and isetShowByIP

Similar to the **dsetShow** command, the wireless handset outputs its specific hardware ID (see **dsetShow**) and alias IP, not the physical IP address. The FW version has a different format <Version>.<Issue> in this output.

In the following example, the telephone with TN 062-02 is the WLAN Handset 2211.

```
-> isetShow
Set Information
---------------
IP Address Type RegType State Up Time Set-TN Regd-TN
---------- ---- ----- ---- ----- ----- -------
192.168.10.100 i2004 Regular online 4 22:59:22 061-00
061-00

HWID FWVsn UNIStimVsn SrcPort DstPort
------------------ ---- -------- ----- -----
180060387641c76600 0602B59 2.8 5100 5000
```


Copyright © 2004–2008 Nortel Networks

```
IP Address Type RegType State Up Time Set-TN Regd-TN
---------- ---- ----- ---- ----- ----- -------
192.168.10.200 i2004 Regular online 0 02:03:22 062-02
062-02

HWID FWVsn UNIStimVsn SrcPort DstPort
---------------- ----- ------- ----- ------
3000907a017e476607 097.021 2.6 5100 5000
```

umsKernalJobsShow and umsUpgradeAll

The umsKernalJobsShow and umsUpgradeAll commands cannot be used to monitor and originate software upgrades for wireless handsets since the wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem. For information about how to monitor and originate the software upgrade, see the documentation for the TFTP server used by the wireless handsets.

umsPolicyShow and umsUpdatePolicy

The IP Phone 2004 policy used in these commands is not applicable to handsets, even though they are configured as IP Phones 2004 in the IP Line software. The wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem.

usiLibTrace

The **usiLibTrace** utility can be used to monitor UNIStim messages from the wireless handsets by entering the alias IP address, not the wireless handset physical IP address.

```
-> usiLibTraceOn "192.168.10.200", 255, 255
value = 0 = 0x0
```

Determining alias IP addresses

When diagnosing network problems, (for example, to ping the wireless handset), it is useful to know the mapping between the alias IP addresses as displayed by various Call Server commands and the physical IP address of the wireless handset. There is no single command that provides this information; however, the administrator can determine it in two ways:

1. If the wireless handset IP address is statically configured, the administrator can look at the IP address of the wireless handset using the Admin menu, which is available when the wireless handset is powered on.
2. After the wireless handset is operating and in standby mode, the administrator can look at the User Preferences menu to find the alias IP address of the wireless handset.

Copyright © 2004–2008 Nortel Networks

For more information, see *WLAN Handsets Fundamentals (NN43001-505)*, .

Troubleshooting coverage issues

Coverage issues are best resolved by adding and relocating APs as required. Overlap issues can be resolved by reassigning channels to the APs or by relocating the APs. For more information, see "Troubleshooting WLAN IP Telephony installations" (page 167).

Before calling Nortel Technical Support

To facilitate the handling of the call, obtain the following information and have it available when placing a call to Nortel Technical Support:

- software versions on the wireless infrastructure, such as the APs
- pre-installation site survey, including typical network information and the wireless site survey information from the site survey tool such as the Nortel Site Survey Tool
- paper-based layout of AP placement
- a more refined site survey of the area having issues using the wireless handset in Site Survey mode
- list of the PBX and LTPS software versions, including a list of patches
- WLAN IP Telephony Manager 2245 and handset firmware versions
- WLAN IP Telephony Manager 2245 configuration menu screen captures
- any error messages displayed in the Error Status screen of the System Status Menu of the WLAN IP Telephony Manager 2245
- any error messages displayed on the handset display screen
- content of the Syslog Server (if using)
- log of the DHCP Server (if available), if using DHCP

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

Appendix WLAN Application Gateway 2246

This appendix contains information about the following topics:

- "Introduction" (page 141)
- "Third-party applications" (page 144)
- "Installation" (page 145)
- "Configuration" (page 147)
- "Continuing configuration through Telnet" (page 153)
- "System status" (page 158)
- "Certification testing" (page 161)
- "Software" (page 161)
- "Planning Worksheet for Handsets" (page 164)
- "Free the serial port for administrative purposes" (page 165)

Introduction

With the optional WLAN Application Gateway 2246, third-party applications can communicate directly with a maximum of 10,000 handsets. With the WLAN Application Gateway 2246, users can retrieve and respond to information using their wireless handsets.

The WLAN Application Gateway 2246 is available in several scaled capacity levels. The base unit NTTQ65AB enables 64 wireless handsets.

Table 17
Model numbers with maximum number of users

Model number	Maximum number of users
NTTQ65AB	64
NTTQ65BA	128

Copyright © 2004–2008 Nortel Networks

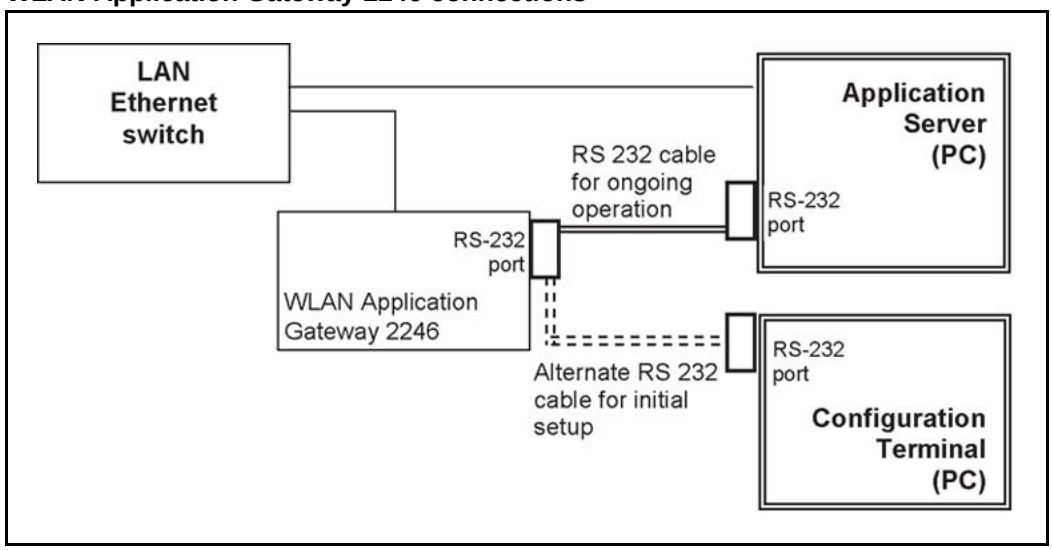
Table 17
Model numbers with maximum number of users (cont'd.)

Model number	Maximum number of users
NTTQ65CA	256
NTTQ65DA	512
NTTQ65EA	1024
NTTQ65FA	10000

In Figure 23 "WLAN Application Gateway 2246 connections" (page 142), a WLAN Application Gateway 2246 is connected to the site LAN through an Ethernet switch. The connection to the Application Server can be accomplished by a direct connection (RS-232) or through the Ethernet connection. Only one of these connections can be used at one time.

The IP address of the WLAN Application Gateway 2246 must be configured during initial configuration. After the IP address is established, the WLAN Application Gateway 2246 can be accessed by the Application Server through the RS-232 port or through the LAN using Telnet.

Figure 23
WLAN Application Gateway 2246 connections

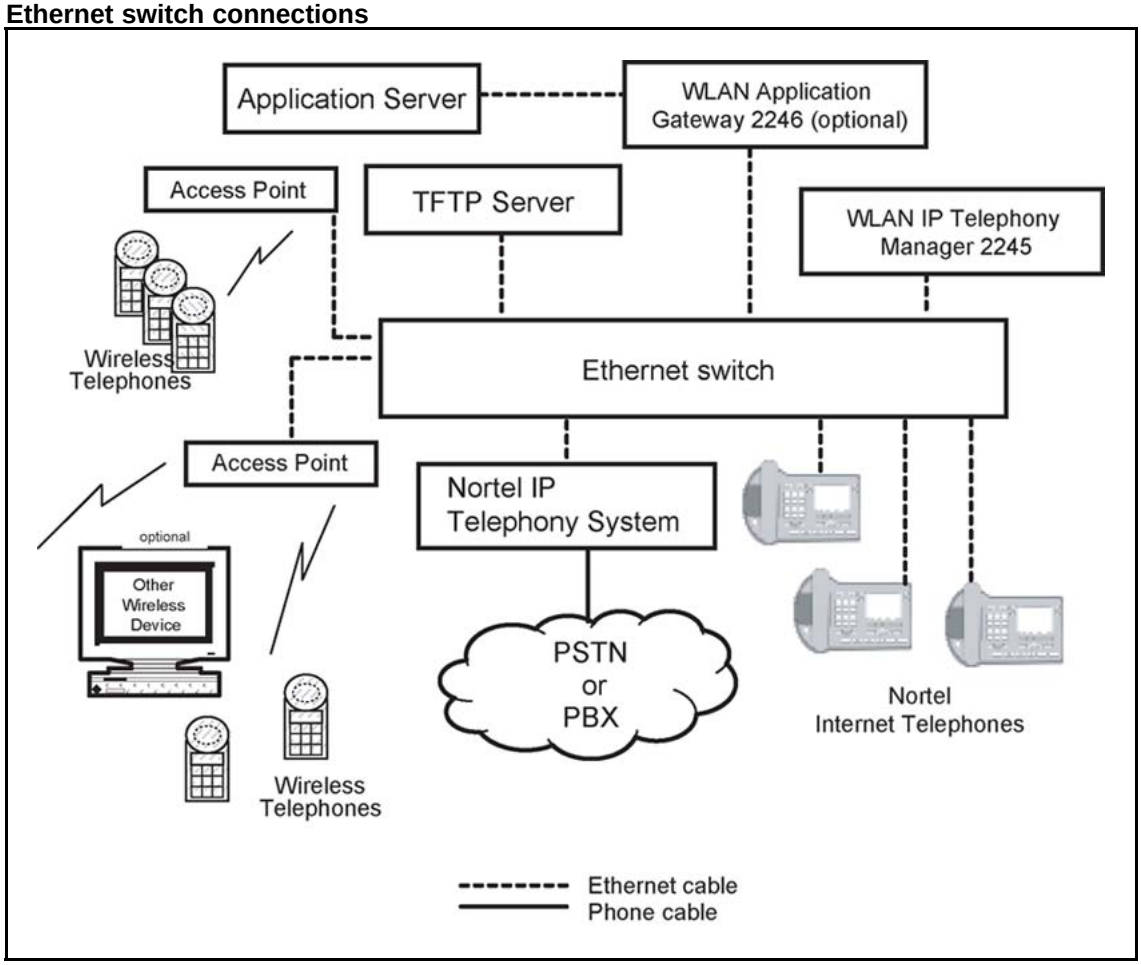


System overview

At a typical site, the WLAN Application Gateway 2246 is connected to the Ethernet switch through an RJ-45CAT 5 cable. The Application Server is connected through the RS-232 port. The client's system can include a LAN and its Application Server with a TAP connection to a communications device such as a paging controller.

Copyright © 2004–2008 Nortel Networks

Figure 24
Ethernet switch connections



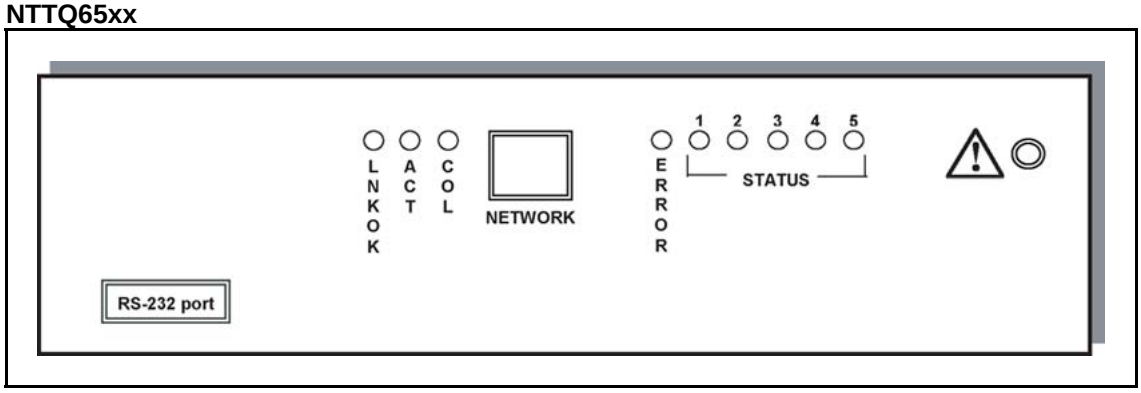
Front panel

The WLAN Application Gateway 2246 models have similar front panel indicators. See Figure 25 "NTTQ65xx" (page 144).

The NTTQ65xx is available in scaled increments to support up to 10 000 users.

Copyright © 2004–2008 Nortel Networks

Figure 25
NTTQ65xx



- Network Link LEDs
  - **(L)NKOK**—lit when there is a network connection, (for example, LINK OK).
  - **(A)CT**—lit if there is system activity.
  - **(C)OL**—lit if there are network collisions.
  - **(E)RROR**—lit when the system has detected an error.
- Status LEDs—indicate system messages and status. See Figure 25 "NTTQ65xx" (page 144).
  - **1**—heartbeat, indicates the WLAN Application Gateway 2246 is running
  - **2, 3, and 4**—currently unused
  - **5**—System master

Third-party applications

The WLAN Application Gateway 2246 enables third-party software applications to communicate with the wireless telephones. Users can receive and retrieve important information from external systems. Some examples of applications in various markets are as follows:

Health care:

- access patient pharmaceutical records
- receive text messages from nurse call systems
- receive e-mail from remote test labs

Retail:

- look up merchandise prices
- access inventory

Copyright © 2004–2008 Nortel Networks

Manufacturing:

- relay alarms to handsets from malfunctioning equipment
- enable managers to monitor production output

Call Centers:

- review queue statistics
- receive alarms when metrics exceed thresholds

Nurse-call systems

In the health care market, the following nurse-call system manufacturers have applications known to be compatible with the WLAN Application Gateway 2246:

- Dukane Corporation
- Emergin WirelessOffice
- Globestar
- Indyme Corporation
- Jeron Nurse Call
- OnSite Communications
- Rauland Nurse Call
- SoloTraxx
- Wescom Nurse Call

Installation

Installing with a new system

If this is a new system installation, complete Procedure 12 “Installing the WLAN Application Gateway 2246” (page 146) when the rest of the system is tested.

Installing in an existing system

If the WLAN Application Gateway 2246 is being added to an existing system, the entire system must be reset before the WLAN Application Gateway 2246 can be used.

Follow the steps in Procedure 12 “Installing the WLAN Application Gateway 2246” (page 146) to install the WLAN Application Gateway 2246.

Copyright © 2004–2008 Nortel Networks

Procedure 12
Installing the WLAN Application Gateway 2246

Step	Action
1	Place the WLAN Application Gateway 2246 on a shelf or convenient location.

ATTENTION
The WLAN Application Gateway 2246 is physically connected to the Ethernet switch and can be placed in any convenient location within 325 ft (100 m) of the switch. It can also be rack-mounted.

Step	Action
2	Connect the power plug from the WLAN Application Gateway 2246 power adapter to the power jack on the front (or rear) of the box.

ATTENTION
IMPORTANT
Use only the power adapter provided by Nortel.

Step	Action
3	Plug the power adapter into an outlet or outlet strip.
4	Apply power to the WLAN Application Gateway 2246.
5	Ensure that the ERROR LED is off and LED 1 is blinking.

--End--

Configuring the WLAN Application Gateway 2246 IP address

You must connect to the WLAN Application Gateway 2246 through a serial connection to configure the IP address and the network parameters. After this is done, you can perform administration and further configuration through a Telnet connection using the Administration Console.

Follow the steps in Procedure 13 “Connecting to the WLAN Application Gateway 2246 through a serial port” (page 146) to make a serial connection to the WLAN Application Gateway 2246.

Procedure 13
Connecting to the WLAN Application Gateway 2246 through a serial port

Step	Action
1	Using a DB-9 female, null-modem cable, connect the WLAN Application Gateway 2246 to the serial port of a terminal or PC.
2	Run a terminal emulation program (such as HyperTerminal) or use a VT-100 terminal with the following configuration: • Bits per second: 9600 • Data bits: 8

Copyright © 2004–2008 Nortel Networks

- Parity: None
- Stop bits: 1
- Flow control: None

ATTENTION
If you use Windows 2000, you must install Service Pack 2 to enable the use of HyperTerminal™.

3 Reset the system.

The following appears on the terminal display:

04830130

4 Type the following command using the terminal or PC keyboard:

```
0255CC [CTRL M] [CTRL J]
```

The command does not display on the screen as it is typed.

The **Login** prompt appears. If an error is made when entering the command string, the message `Ill Formed Packet` appears. It appears as a series of numbers followed by some form of the typed command. If this occurs, repeat Step 3 and Step 4.

5 Enter the default logon name and the default password:**admin**
admin

admin
admin

The logon name and password are case-sensitive.

The **NetLink OAI System** screen appears. This screen, the main menu screen of the Administration Console, displays the factory-default name of the WLAN Application Gateway 2246 to which the serial port is connected

--End--

Next, configure the WLAN Application Gateway (including IP address) by following the steps in the “Task summary list” (page 148).

Configuration

The NetLink OAI System screen is the main menu of the Administration Console. Use this screen to configure the WLAN Application Gateway 2246.

Administration console navigation

Use the keys described in Table 18 "Administration console navigation" (page 148) to move around the Administration console screens.

Copyright © 2004–2008 Nortel Networks

Table 18
Administration console navigation

To perform this function	Press
Select function from menu	Arrow keys to highlight the selection. Press **Enter**.
Display menu associated with highlighted field	**Enter**. The Enter key displays the options associated with an item or allows an entry to be typed into the field.
Exit screen	**Esc**. Press the Esc key to return to the previous screen.
Move one line up	Corresponding arrow key.
Move one line down	
Move one field to the left	
Move one field to the right	
Scroll	If a screen has more lines of information than can be displayed at once, the text is wrapped. The scroll feature uses the arrow keys. Press the down arrow key at the last line to move the cursor to the top line. Press the up arrow key at the top line to move the cursor to the last line.

The top line of each screen of the Administration Console displays the hostname and IP address of the WLAN Application Gateway 2246.

Task summary list

Complete the following tasks to configure the WLAN Application Gateway 2246:

Step	Action
1	Select the **OAI Box Configuration** option to configure the system type. See “Configuring the OAI Box” (page 149).
2	Select the **Network Configuration** option to configure the Network settings. See “Configuring network parameters” (page 149).
3	Select the **Telephone Line Configuration** option to configure the handsets . See “Configuring the Telephone Line” (page 154).
4	Select the **Feature Programming** option to configure the function sequence that activates the application. See “Feature programming” (page 157).

--End--

Copyright © 2004–2008 Nortel Networks

Configuring the OAI Box

Follow the steps in Procedure 14 “Configure the system type from the OAI Box Configuration option” (page 149) to configure the system type.

Procedure 14
Configure the system type from the OAI Box Configuration option

Step	Action
1	From the **NetLink OAI System** screen, select **OAI Box Configuration**. This option does not appear unless Use NetLink GW with mogX00 is configured to Yes, which is the default.
2	Enter the configuration information for the WLAN Application Gateway 2246 (provided by the network administrator). • **Use NetLink GW with mogX00**—change this option to **No**. • **TFTP Download Master**—enter the IP address of the TFTP Server. • **Maintenance Lock**—the system sets this option to **Yes** after maintenance activities are performed that require a reset. This option cannot be changed. It is automatically set. Reset the system at exit to clear Maintenance Lock. Maintenance Lock prevents any new calls from starting. • **Reset System**—if this option is set to **Yes**, the WLAN Application Gateway 2246 is reset after pressing **ENTER**. • **Reset All Systems**—not applicable.
3	Press **Esc** on the keyboard to return to the **NetLink OAI System** screen.
	--End--

Configuring network parameters

Follow the steps in Procedure 15 “Configuring the network” (page 149) to configure network parameters, including IP address.

Procedure 15
Configuring the network

Step	Action
1	From the **NetLink OAI System** screen, select **Network Configuration**.
2	Enter the configuration information for the WLAN Application Gateway 2246, as provided by the network administrator.

Copyright © 2004–2008 Nortel Networks

- **Ethernet Address**—this is the MAC address of the WLAN Application Gateway 2246. This address is set at the factory.
- **IP Address**—enter the complete IP address for the WLAN Application Gateway 2246, including digits and periods. Do not use DHCP. The IP address can be changed after initial configuration.
- **Hostname**—the default host name can be changed. This is the name of the WLAN Application Gateway 2246 to which connection is made. This name is for identification purposes only. Spaces cannot be entered in this field.
- **Subnet Mask**—Enter the subnet mask defined by the network administrator.
- **Default Router**—DHCP or static IP address.
- **Allow Telnet Connections**—Enter **Y** (Yes) to allow connection to the WLAN Application Gateway 2246 through Telnet. Enter **N** (No) if no Telnet connection is allowed.
- **Allow FTP Connections**—Yes or No (NTTQ65xx models only).
- **DNS server and DNS domain**—these settings are used to configure Domain Name Services (DNS). (These settings can also be configured as DHCP. This causes the DHCP client in the WLAN Application Gateway 2246 to attempt to automatically obtain the correct configuration from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP).
- **WINS servers**—these settings are used for Windows Internet Name Services (WINS). (These settings can also be configured as DHCP. This causes the DHCP client in the WLAN Application Gateway 2246 to attempt to automatically obtain the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.) When WINS is configured properly, the WLAN Application Gateway 2246 can translate hostnames to IP addresses. When using Telnet, it is also possible to access the WLAN Application Gateway 2246 using its hostname instead of the IP address.
- **Logging**—can be configured to **Syslog** or **NONE**.
- **Log server**—enter the IP address or hostname of the Syslog Server on the network if Syslog is configured. The WLAN Application Gateway 2246 writes Syslog format diagnostic messages to the Syslog Server.
- **SNTP server**—can be configured as a hostname, IP address, or NONE. The SNTP server is a Simple Network Time server. The WLAN Application Gateway 2246 obtains the

Copyright © 2004–2008 Nortel Networks

current date and time from the SNTP server and tags syslog messages with the date.

- **IGMP Enabled**—configure as **Yes** or **No**. IGMP is Internet Group Routing Protocol. **IGMP Enabled** allows the WLAN Application Gateway 2246 to join multicast groups. Enable this option if the network switch connected to the WLAN Application Gateway 2246 requires IGMP for multicast traffic to be forwarded.
- **Maintenance Lock**—the system sets this option to **Yes** after maintenance activities are performed that require a reset. This option cannot be changed. It is automatically set. Reset the system at exit to clear Maintenance Lock. Maintenance Lock prevents any new calls from starting.
- Press **ESC** to return to the **NetLink OAI System** screen.
- Reset the WLAN Application Gateway 2246.

--End--

Connecting to the LAN

Follow the steps in Procedure 16 “Connecting the WLAN Application Gateway 2246 to the LAN” (page 151) to connect the WLAN Application Gateway 2246 to the LAN.

Procedure 16
Connecting the WLAN Application Gateway 2246 to the LAN

Step	Action
1	Using an RJ-45 cable, connect the NETWORK port of the WLAN Application Gateway 2246 to the connecting port on the Ethernet switch.
2	Power up the entire system.

--End--

All components cycle through their usual diagnostic routine.

Connecting to the Application Server

Some applications can require a LAN connection between the Application Server and the WLAN Application Gateway 2246. If the applications do not require a LAN connection, use the RS-232 port connection. In some situations, a modem is connected to be used for remote administration of the WLAN Application Gateway 2246.

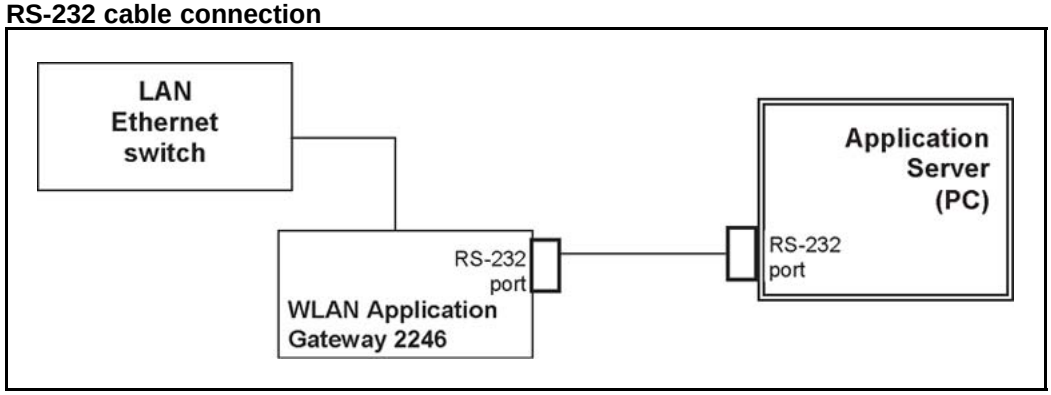
Copyright © 2004–2008 Nortel Networks

Connect to the Application Server through an RS-232 port

Some applications or systems can require an RS-232 connection between the Application Server and the WLAN Application Gateway 2246. If the applications have the ability to communicate messages over TCP/IP, and do not require a serial connection, the RS-232 cabling is not required. In that case, the LAN connection (port 5456) through the Ethernet switch can be used for the applications.

Connect the Application Server to the WLAN Application Gateway 2246 serial port by using a cable that conforms to RS-232 standards for DTE-to-DTE connections (null modem cable).

Figure 26
RS-232 cable connection



The WLAN Application Gateway 2246 uses the following pins on the connector.

Table 19
Pins on the connector

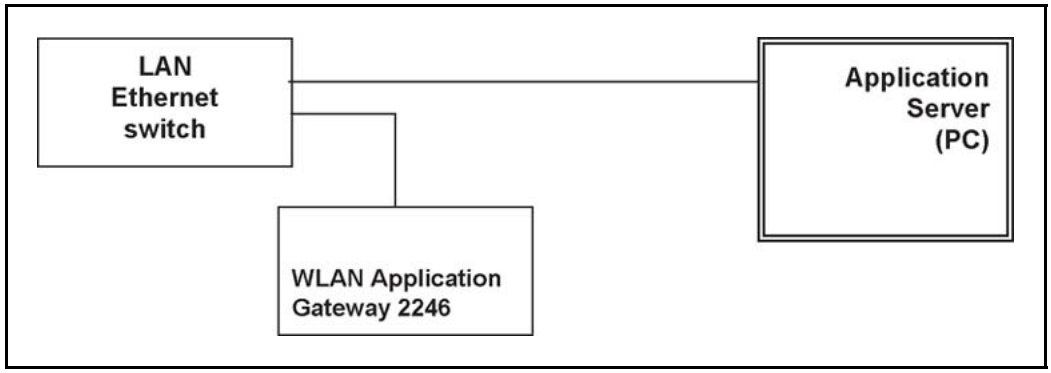
Pin	Function
1	Carrier Detect
2	Data OAI Receives
3	Data OAI Transmits
5	Ground
7	Ready to Send
8	Clear to Send

Connect to the Application Server through the LAN

The IP address must be configured for the WLAN Application Gateway 2246 to function on the LAN. Follow the application instructions to identify the WLAN Application Gateway 2246 to the application.

Copyright © 2004–2008 Nortel Networks

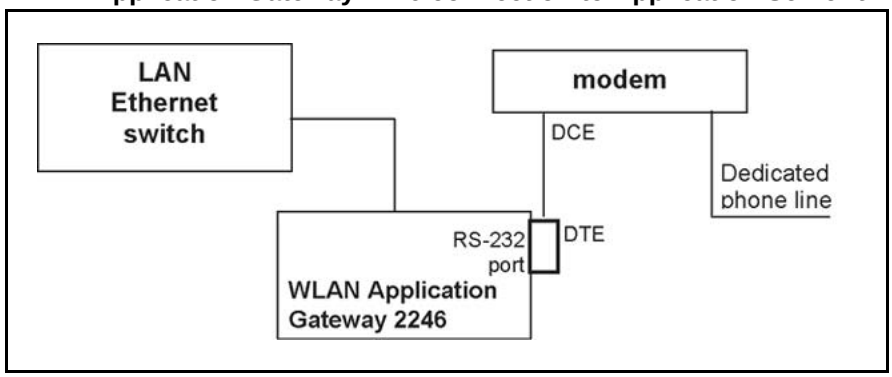
Figure 27
WLAN Application Gateway 2246 connection to Application Server through the LAN



Connect to Application Server through a modem

Connect the modem to the Gateway serial port using a cable that conforms to RS-232 standards for DTE-to-DCE connections. See Figure 28 "WLAN Application Gateway 2246 connection to Application Server through a modem" (page 153).

Figure 28
WLAN Application Gateway 2246 connection to Application Server through a modem



Continuing configuration through Telnet

After the IP address for the WLAN Application Gateway 2246 is configured, the WLAN Application Gateway 2246 reset and connected to the LAN and the Application Server, Telnet can be used to continue the WLAN Application Gateway 2246 configuration.

Connecting through Telnet

Connection to the WLAN Application Gateway 2246 can be done through the network using Telnet. Telnet can only be used after the WLAN Application Gateway 2246 IP address is configured.

Copyright © 2004–2008 Nortel Networks

The Telnet method of connection is used for routine maintenance of the system for both local and remote administration, depending on the network.

Follow the steps in Procedure 17 “Connecting to a WLAN Application Gateway 2246 through Telnet” (page 154) to connect to a WLAN Application Gateway 2246 through Telnet.

Procedure 17
Connecting to a WLAN Application Gateway 2246 through Telnet

Step	Action
1	Run a Telnet session to the IP address of the WLAN Application Gateway 2246.
2	Log in to the WLAN Application Gateway 2246. The **NetLink OAI System** screen appears. Because the WLAN Application Gateway 2246 is initially configured, the **NetLink OAI System** screen now has some different options displayed.

--End--

When the configuration procedure is complete, the NetLink OAI System screen adds a Feature Programming option. Also, the OAI Line Configuration option is replaced by a Telephone Line Configuration option.

Configuring the Telephone Line

Each handset that uses the application features must be configured with its line number and MAC address. The name and extension number of the handset user can be entered. Obtain this information from the handset Planning Worksheet. See “Planning Worksheet for Handsets” (page 164).

The handsets require special configuration. This can include configuring options on the DHCP server or on the handset to allow it to communicate with the WLAN Application Gateway 2246. Be sure these setting are correct. For more information, see *WLAN Handsets Fundamentals (NN43001-505)*, .

The system does not allow the same handset to register to two different lines. Press **Esc** to cancel any unwanted transaction.

Follow the steps in Procedure 18 “Configuring a telephone line” (page 155) to configure the telephone lines for the application.

Copyright © 2004–2008 Nortel Networks

Procedure 18
Configuring a telephone line

Step	Action
1	From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.
2	At the Telephone Line Configuration screen, use the arrow keys to navigate to the **Name** and **Extension** fields.
3	Enter the associated data for the wireless handsets. • **MAC Address**—the MAC address is printed on the sticker underneath the battery on the handset. It can also be displayed on the handset by turning off the wireless handset, and then pressing and holding the Power On/Start Call button. The MAC address appears on the first line of the wireless handset display (12 characters). The MAC address must be manually entered by typing the entire address, including digits and colons. • **Name**—enter the user name assigned to the wireless handset. This is for record keeping only; it does not communicate the name to the Call Server or the handset. • **Extension**—enter the extension number assigned to the handset. This is for record keeping only; it does not communicate the extension number to the Call Server or the handset.
4	Write the MAC address on the Wireless Handset Planning Worksheet. See "Planning Worksheet for Handsets" (page 164).
5	Repeat step 4, step 5, and step 6 for each wireless handset to be added or changed.
6	Press **Esc** to return to the **NetLink OAI System** screen.

--End--

Deleting a handset

Follow the steps in Procedure 19 "Deleting a handset" (page 155) to delete a WLAN IP Telephony Manager.

Procedure 19
Deleting a handset

Step	Action
1	From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.

Copyright © 2004–2008 Nortel Networks

The **Telephone Line Configuration** screen displays.

2 Use the arrow keys to highlight the line to be deleted.

3 Press **D** to delete the handset information.

4 Press **Y** to accept changes.

5 Press **Esc** to return to the **NetLink OAI System** screen.

--End--

Searching for a handset

While in the Telephone Line Configuration or the Telephone Line Status screens, a search hot key is available.

Follow the steps in Procedure 20 “Searching for a handset” (page 156) to search for a handset.

Procedure 20
Searching for a handset

Step	Action
1	From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.
2	At the **Telephone Line Configuration** screen, select the field to use as the search key (**MAC Address**, **Name**, or **Extension**),
3	Press **S** to display a search screen dialog box.
4	Type an appropriate search string.
5	Press **Enter**. The success or failure of the search appears at the bottom of the screen.
6	Continue to change the search string for different search criteria or exit by pressing the **Esc** key.

--End--

The first line of the Telephone Line Configuration or Telephone Line Status screen displays the line in which the search match is found.

Successful searches always have the first found match at the top of the list.

Partial strings match the beginning of strings. For example, a search for extension 10 matches extensions 10, 100, 1000, and so on, but does not match 010.

Copyright © 2004–2008 Nortel Networks

Feature programming

The application function is accessed in the handset by pressing the FCN button plus a second button. The button used to access the application feature from the wireless handset is configured through the Feature Programming option.

FCN 1-6 are hard-coded. If the application function is programmed to use FCN 1-6, the hard-coded function is overridden. Nortel recommends using 7, 8, or 9 for the application function.

Follow the steps in Procedure 21 “Programming a feature” (page 157) to program an application feature for the wireless handsets.

Procedure 21
Programming a feature

Step	Action
1	From the **NetLink OAI System** screen, select **Feature Programming** and press **Enter**.
2	At the Feature Programming screen , use the arrow keys to select the function number 7, 8, or 9 to associate with the application.
3	Type any label up to six characters. The label you type here appears on the handset telephone display screen next to the assigned number on the FCN menu.

--End--

Setting or changing a password

You can configure a unique password for the WLAN Application Gateway 2246. The password restricts access to administrative functions of the device.

WARNING
Record the password and store it in a safe place. If the password is lost or forgotten, contact Nortel Technical Support.

Follow the steps in Procedure 22 “Setting or changing a password” (page 158) to configure or change a password on the WLAN Application Gateway 2246.

Copyright © 2004–2008 Nortel Networks

Procedure 22
Setting or changing a password

Step	Action
1	From the **NetLink OAI System** screen, select **Change Password** and press **Enter**. The Change Password screen displays. An asterisk (*) indicates an item that is not applicable.
2	Enter the default password: `admin`
3	Follow the prompts to configure a new password.

--End--

System status

Use the steps in Procedure 23 “Viewing system status” (page 158) to view the status of the system.

Procedure 23
Viewing system status

Step	Action
1	From the **NetLink OAI System** screen, select the **System Status Menu** option.
2	At the **Systems Status Menu** screen, select from the following options: • **Application Active**—*Yes* appears if the application is communicating correctly with the WLAN Application Gateway 2246. *No* appears if the application is not connected. This field is read-only and changes dynamically. • **Error Status**—The only application-specific error is **No ECP heartbeat**, which means the application failed to send a heartbeat to the WLAN Application Gateway 2246. • **Network Status**—information about the connection to the LAN. See “Network status” (page 159). • **Software Versions**—lists the software versions currently running on the WLAN Application Gateway 2246. See “Software versions” (page 160). • *** Telephone Line Status**—provides information about the functioning of each wireless handset registered to the WLAN

Copyright © 2004–2008 Nortel Networks

Application Gateway 2246. See “Telephone line status” (page 160).

--End--

Network status

The WLAN Application Gateway 2246 is connected to the Ethernet network, referred to as the LAN. The information about this connection displayed on the Network Status screen.

The following information appears at the top of the screen:

- **Ethernet Address**—MAC address of the WLAN Application Gateway 2246 (hexadecimal).
- **Stats Time Period**—the length of time the statistics are accumulating in the **Pkts** and **Bytes** columns. This is either the system uptime, or the time that has elapsed since a user pressed **C=Clear** while viewing this display.
- **User Time Period**—the length of time (in seconds) that statistics accumulate in the **Userpkts** column before resetting to zero. When troubleshooting a problem, use this setting to isolate statistics for a given time period (for example, one hour). This is the only field in this screen that can be changed by the user.

The rest of the display is a table of Ethernet statistics. The Pkts and User Pkts columns list the count of Ethernet packets received or transmitted. The Bytes column is the count of bytes received or transmitted during the amount of time indicated by the Stats Time Period.

- **RX**—number of packets and bytes received addressed to the WLAN Application Gateway 2246.
- **RX Broadcast**—the number of broadcast packets and bytes received.
- **RX Multicast**—the number of packets and bytes received with the multicast address. (A multicast message is sent to more than one destination on the network.)
- **RX Not For Us**—the number of multicast packets and bytes received that were not for the WLAN Application Gateway 2246.
- **TX**—the total number of packets and bytes transmitted.
- **Interrupts**—the number of times the Ethernet controller signals the microprocessor that it has received or sent a packet.

Copyright © 2004–2008 Nortel Networks

- **Collisions**—the number of times the Ethernet controller attempts to send a packet, but another device on the network transmitted at the same time, corrupting the transmission.
- **Collision Drops**—the number of packets the Ethernet controller discards, because there were over sixteen collisions. After sixteen collisions, the Ethernet controller hardware discards the current packet and attempts to send the next packet in its buffer.
- **CRC Errors**—the number of packets discarded by the Ethernet controller, because of a Cyclic Redundancy Check (CRC) error.

Viewing the network status

From the **System Status Menu** screen, select **Network Status**.

The Network Status screen displays information about the Ethernet network. This information can help troubleshoot network problems.

Software versions

Each WLAN Application Gateway 2246 and handset runs software that is controlled and maintained through versioning. The Software Versions screen provides information about the version currently running on the components. This information helps determine if the most recent version of software is running, and assists Nortel Technical Support in troubleshooting software problems.

Viewing software versions

From the **System Status Menu** screen, select **Software Versions**.

Telephone line status

The Telephone Line Status screen displays which wireless handsets are communicating with the WLAN Application Gateway 2246.

The following information appears on the **Telephone Line Status** screen:

- **WT MAC**—the MAC address of the handset that is entered when the wireless handset is configured.
- **NameExtension**—these fields contain the data entered at configuration.
- **Phone**—**No ChkIn** indicates the handset is not using the application function. **ChkIn** indicates the handset is communicating with the WLAN Application Gateway 2246.

Viewing telephone line status

From the System Status Menu screen, select **Telephone Line Status**.

Copyright © 2004–2008 Nortel Networks

The WLAN Application Gateway 2246 displays up to 16 telephone lines at one time. Move to the next group of 16 lines by using the arrow keys.

Certification testing

The following sections provide information about certification testing.

WLAN Application Gateway 2246 certification

After the WLAN Application Gateway 2246 is properly connected to the Application Server, LED 1 blinks.

Wireless handset certification

The procedure for certification of wireless handsets is different depending on whether you are installing the WLAN Application Gateway 2246 on a new system or an existing system.

WLAN Application Gateway 2246 installation on new system

If this is a new system installation, continue with handset registration and Call Server programming. When the wireless handset installation is complete, perform the usual voice and coverage tests.

WLAN Application Gateway 2246 installation on existing system

Follow the steps in Procedure 24 “Certifying wireless handsets on an existing system” (page 161) to certify the wireless handsets on an existing system.

Procedure 24
Certifying wireless handsets on an existing system

Step	Action
1	Place a test call.
2	Test the features on each handset to ensure the system is working properly.
3	Test the application on each handset.
4	Consult the application provider for specific test procedures.

--End--

Software

The WLAN Application Gateway 2246 and the handset use proprietary software programs. The software versions that are running on the system components can be displayed through the **System Status** screen.

Nortel provides information about software updates, and how to obtain the software (for example, downloading from the Nortel Web site).

Copyright © 2004–2008 Nortel Networks

Software updates

After obtaining the software updates from Nortel, they must be transferred to the appropriate location in the LAN. This enables the corresponding system components to access and update their software. The FTP (File Transfer Protocol) method of transfer is used.

In the WLAN Application Gateway 2246, the flash file system has the following files:

Table 20
Software files

File name	Description
config.bin	OAI box configuration
fnctla.bin	functional code
oaiptlst.bin	phone list configuration
oaipttlsb.bin	redundant phone list configuration

Nortel periodically upgrades the fnctla.bin file, which is the only file downloaded. The other files are configuration files and their names are provided for information and backup purposes.

Obtain software using FTP

When using FTP, a host system is used to connect to a remote system. In this example, the host is the client and the server is the WLAN Application Gateway 2246. The put command means to copy the files from the host to the remote system.

ATTENTION
FTP commands vary with the particular FTP program used. Use the following steps as a general guide but be aware that an FTP program can use different terms to describe the procedure.

Follow the steps in Procedure 25 “Transferring the software using FTP” (page 162) to transfer the software using FTP.

Procedure 25
Transferring the software using FTP

Step	Action
1	Navigate to the **OAI Box Configuration** screen and place the system in Maintenance Lock before proceeding with the FTP procedure. This prevents new calls from starting. No calls can be in progress during the FTP procedure.
2	Connect to the WLAN Application Gateway 2246 using the command:

Copyright © 2004–2008 Nortel Networks

FTP <hostname>
OR
FTP <IP address>.

3 Log on using the default administrator logon and password:
admin
admin

4 At the FTP prompt, type **binary**.

5 At the FTP prompt, rename and transfer the functional code file to the client server or WLAN Application Gateway 2246.

put **mog700.bin fnctla.bin**

where

MOG700.bin is the downloaded file.
fnctla.bin is the new name of the file.

6 After the file transfer is complete, use the **Quit** command to quit FTP.

7 Navigate to the **NetLink OAI System** screen for the WLAN Application Gateway 2246

8 Select **System Status**.

9 Select **Software Versions** to verify that software versions for the WLAN Application Gateway 2246 are correct.

10 Reset the system through the **OAI Box Configuration** screen in order to restore Maintenance Lock to N.

--End--

ATTENTION
You can use a GUI FTP client instead of the described command line FTP procedure.

TFTP software updates Systems

The WLAN Application Gateway 2246 uses proprietary software programs. You can display the software versions running on the system components through the WLAN Application Gateway 2246 System Status screen.

Nortel provides information about software updates and how to obtain the software (for example, downloading from the Nortel Web site).

Follow the steps in Procedure 26 “Loading software updates” (page 164) to load software updates.

Copyright © 2004–2008 Nortel Networks

Procedure 26
Loading software updates

Step	Action
1	Install a TFTP Server on a LAN-connected system.
2	Consult the server vendor's documentation for information about TFTP.
3	After obtaining the software update from Nortel, load the software in a location that is accessible by the TFTP program.
4	To configure the host and start the download, from the **NetLink OAI System** screen, select the **TFTP Server Download Configuration** option.
5	Enter the TFTP Server hostname.
6	Use the arrow keys to move the cursor to the **Begin TFTP Download** option.
7	Press **Enter** to begin the download. The code downloads into the WLAN Application Gateway 2246.

--End--

Planning Worksheet for Handsets

Copy and complete the worksheet in Table 21 "Handset Planning Worksheet" (page 164) to track parameters for each handset.

Table 21
Handset Planning Worksheet

OAI Port	MAC Address	User Name	Dialing Ext.	IP Address (if static)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Copyright © 2004–2008 Nortel Networks

Table 21
Handset Planning Worksheet (cont'd.)

OAI Port	MAC Address	User Name	Dialing Ext.	IP Address (if static)
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

Free the serial port for administrative purposes

If the serial port is being used as the primary communication link with the Application Server, you must enter the OAI command to free the serial port to allow it to be used for administrative purposes, such as changing the IP address of the WLAN Application Gateway 2246.

To free the serial port to allow it to be used for administrative purposes, follow the steps in Procedure 13 "Connecting to the WLAN Application Gateway 2246 through a serial port" (page 146).

After configuring the WLAN Application Gateway 2246, perform the following steps to again use the serial port as the communication link with the Application Server.

Procedure 27
Using the serial port as the Application Server communication link

Copyright © 2004–2008 Nortel Networks

Step	Action
1	Disconnect the terminal or PC from the serial port on the WLAN Application Gateway 2246.
2	Reconnect the communication cable between the WLAN Application Gateway 2246 and the Application Server.
3	Reset the system.
	--End--

Normal communication between the Application Server and WLAN Application Gateway 2246 commences.

Copyright © 2004–2008 Nortel Networks

Appendix Troubleshooting WLAN IP Telephony installations

This appendix contains information required for troubleshooting and diagnosing of a WLAN IP Telephony installation, including the following topics:

- "Site data-gathering tables" (page 167)
- "Product-specific configuration" (page 169)
- "WLAN specific configuration" (page 171)
- "General WLAN configuration" (page 176)
- "DHCP server options" (page 177)
- "DHCP options" (page 178)
- "Quality of Service checklist for voice over WLAN applications" (page 184)
- "Troubleshooting" (page 189)
- "Handset error messages" (page 191)
- "Timing information" (page 192)
- "Diagnostic Tools" (page 193)
- "Data capture" (page 206)
- "Capture assert error messages with the Configuration Cradle" (page 211)
- "Network speech levels" (page 212)
- "Reference documents" (page 212)

Site data-gathering tables

The following are examples of site data-gathering tables.

Copyright © 2004–2008 Nortel Networks

Figure 29
System Information table

System Information						
Customer Network (hardware and software)						
Device	Hardware	Software	Device	Qty	Hardware	Software/Firmware
TPS (SS/BCM/IPL)			Wireless Telephone Sets (WTS)			
VGMC (ITG/IPL/SMC)			2245			
AP			2246			
AP Antenna Int/Ext		NA	Wired IP phones			
AP Antenna Pattern		NA				
LAN/Data Switch			TDM phones			
DHCP Server						
TFTP Server						

Figure 30
System History table

System History	
Date of Install:	
Description of recent upgrades or system changes:	
Suspected Trigger event:	
Problem Theories:	
Tests Performed and Conclusions reached:	
Any other Value-Added information:	

Figure 31
Customer Environment table

Customer Environment	
Type of facility (Office, Manufacturing, Retail, Hospital, etc.)	
Name/Description of other wireless products in use at site.	
Was site survey or analysis performed? If so, by whom and when?	
Was WLAN deployment designed for VoIP?	
Other environmental variables?	

Copyright © 2004–2008 Nortel Networks

Figure 32
Attachments: IP Sniffer Trace Captures table

Attachments: IP Sniffer Trace Captures — Wired and Wireless			
File Name	MAC of Phones	How Was Trace Captured?	Trace WEP Key

ATTENTION
Take the wired traces at the mirrored port, to which the 2245 connects, on the Data Switch.

Take the Wireless traces at the Access Points (AP), which are associated with the Wireless Telephony Sets (WTS), on the channels that are used.

Figure 33
Attachments: Other Required table

Attachments: Other Required		
	File Name(s)	Remarks
Network Topology Drawings		
Access Point Configurations		
Data Switch QoS Configurations		
LD 22 ISSP from CS1000 CS		
pdt ISSP from CS1000 SS		
plist from each VGMC		

Product-specific configuration

The following sections provide product-specific configuration information.

Terminal proxy server

Ensure that the system meets the following requirements:

- CS1000 Release 3.0: include the patches identified in the current product bulletin

Copyright © 2004–2008 Nortel Networks

2210, 2211: firmware version 97.070
2245: load 174.027

- CS1000 Release 4.0: include the patches identified in the current product bulletin
  2210, 2211, 2212: firmware version 97.070
  2245: load 174.027
- CS1000 Release 4.5: include the patches identified in the current product bulletin
  2210, 2211, 2212: firmware version 97.070
  2245: load 174.027
- BCM 3.6: requires cumulative patch #3
  2210, 2211: firmware version 97.070
- BCM 3.7
  2210, 2211: firmware version 97.070
- BCM 4.0
  2210, 2211, 2212: firmware version 97.070
- CS2100: requires software version CICMXPM SE09
  Handset firmware version - 97.070

Handsets

For the WLAN Handsets 2210/2211/2212, configure the license code to 010 to download the Nortel UNIStim firmware.

For the WLAN Handsets 6120/6140, configure the Telephony Protocol to 032.

For firmware and documentation, go to www130.nortelnetworks.com.

WLAN IP Telephony Manager 2245

If you have multiple WLAN IP Telephony Manager 2245 units, you must split the alias IP address range to allocate a range to each 2245. Failure to do so causes nonfunctioning handsets because one or more 2245 units cannot allocate alias IP addresses. Without alias IP addresses, the handsets are unable to register with the terminal proxy server (TPS).

Quality of Service

The Differentiated Services Code Point (DSCP) Tag is a Quality of Service (QoS) mechanism for setting relative priorities. Packets are tagged with a DSCP field in the IP header for type of service. Configure the value as a number from 0 to 255; the value can be different for each traffic class listed on the screen. Administrative traffic can have the lowest priority because it does not require voice quality.

Copyright © 2004–2008 Nortel Networks

DSCP tags determine packet priorities for QoS. Nortel recommends the following settings:

WT (In call)—46 (default 4)
WT (Standby)—40 (default 0)
RTP—46 (default 4)
PBX—40 (default 0)
Inter-SVP2—0 (default)

Other networks may use different settings—adjust as needed to match the network.

ATTENTION
IMPORTANT
You must configure the command **mls qos trust dscp** on every on every Cisco switch port, on which a 2245 is installed; otherwise, the DSCP tagging configured on the SVP servers is ignored.

WLAN specific configuration

The following sections provide configuration information for various switches. In this document, WLAN Security Switch means Nortel WLAN Security Switch.

Nortel switches

This section contains configuration information for Nortel switches.

Nortel WLAN Security Switch

The 2350, 2360, and 2380 model switches have the following requirements:

- load 4.1.14
- configure radio-profile voice dtim-interval 3
- configure radio-profile voice active-scan disable (prevents the AP from going off-channel to scan)
- radio-profile voice WMM enabled

Cisco access points and switches

This section contains configuration information for selected Cisco access points and switches.

Cisco Aironet 1200 Series

Ensure that the software is 12.3.7(JA3). This requirement is current as of November 2006 and is subject to change.

Copyright © 2004–2008 Nortel Networks

Configure the following settings:

- dtim-interval 3
- protocol 119 enabled
- less than 10 ms voice latency
- voice WMM enabled

For more information, see the *Cisco Aironet 1200 Series User Guide*, .

Nortel WLAN Security Switch 2270 and the Cisco 4400 Series WLAN Controller

Alpha The 2270 and 4400 infrastructure has the following requirements:

- Turn off aggressive load balancing.
- Disable MAC filtering authentication for voice SSID and use only static WEP (40 or 104 bit) encryption.
- Configure 802.11b radio data rates as follows:
  - 1Mb/s—Mandatory
  - 2Mb/s—Mandatory
  - 5.5Mb/s—Supported
  - 11Mb/s—Supported
- Uncheck enable short preamble.
- Enable Multicast Support on the WLAN Security Switch 2270 to enable use of the PTT feature for Nortel Handsets.
  With the following settings, you can use Multicast for some of the regular SVP server and PBX control traffic:
  Switch > General: Ethernet Multicast Support = Enabled: (2.2)
  Switch > General, Ports: click ports 1 edit on right hand side of the screen and configure Multicast Appliance Mode = Enabled.
- Turn off Rogue AP Detection.
- Turn off AutoRF unless you are running software from Cisco version 4.0.206.0 or later. If you are running version 4.0.206.0 or later, configure the following additional parameters for AutoRF:

Parameter	Setting	Importance
Noise Measurement	3600	Required
Load Measurement	3600	Required
Signal Measurement	3600	Required
Coverage Measurement	3600	Required

- Verify that Idle timer is configured to 300 seconds.

Copyright © 2004–2008 Nortel Networks

- Verify that the AP session timeout is at least 1800 seconds. Nortel recommends that you configure the AP session timeout to 65 534 seconds.
- Verify the following setting:
  2230 AP DTIM = 3
- If there are multiple WLAN Security Switch 2270s installed, which are intended to participate in a single RF mobility group, the following criteria must be met:
  - The RF mobility group name must be same on all 2270s that belong to the RF mobility group.
    The mobility group name is case sensitive.
  - Configure the virtual IP address for virtual interface to a nonroutable address (for example, a fictitious address such as 1.1.1.1). The virtual IP address must be same on all 2270s that belong to the RF mobility group.
  - Manually add each switch to the list of RF mobility group members for each switch.
    This is not a dynamic configuration.
    For example, you have three switches: A, B, and C.
    You must add B and C as members under mobility group configuration for switch A.
    You must add A and C as members under mobility group configuration for switch B.
    You must add A and B as members under mobility group configuration for switch C.
    The above recommendation is true in the case of VoDATA as well.

WLAN Security Switch 2270 notes The following list contains important information about the WLAN Security Switch 2270 and pre-3.2.116.21 code.

- In the 2.0.x code for the WLAN Security Switch 2270, multicast packets are directly handled by the CPU. Nortel Handsets use multicast packets only when the Push-to-talk (PTT) feature is used. Because the CPU handles all multicast packets (control+data) with the 2.0.c code, there can be problems with voice quality for PTT conversations, as well as for regular calls.
  The multicast issues are resolved in the 2.2.x code. With the 2.2.x code, to ease the CPU processing load, multicast packets are off-loaded to another hardware chip within the 2270.
- In the 2.0.x code, if GOLD QoS is enabled for voice SSID, APs can fail to run RRM sampling while packets are processed in the GOLD queue. Therefore, the AutoRFR calculations on the WLAN Security Switch 2270 are further delayed. You must watch out for AutoRF issues in such scenario. If it is a pure voice implementation, you can assign

Copyright © 2004–2008 Nortel Networks

SILVER QoS to voice SSID. This is only a best-effort recommendation. If the voice traffic drops as a result, move back to GOLD QoS for voice.

- The PTT feature does not work in 2.0 code if the WLAN Security Switch 2270 is configured in L2-LWAPP mode. This issue is resolved in the 2.2.x code.
- There is a client-handoff feature in the advanced options in the command line interface (CLI) for release 3.0.107.0.
  For more information, go to www.cisco.com.
  To configure the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the config advanced client-handoff command:
  `config advanced client-handoff <num_of_retries>`
  Default: 0 excessive retries (disabled)
  The command to configure the client handoff to 100 excessive retries is:
  `config advanced client-handoff 100`

ATTENTION
2.x code is not supported. Nortel recommends that sites upgrade to 3.2.116.21 code. Contact Nortel GNTS Technical support to obtain this code—do not download it from the Cisco Web site.

Specific Cisco configuration examples

Table 22 "1230 connected with 2950 and 2245 connected with 2950" (page 174) provides the steps to configure the Cisco Aironet 1230 connected with a Cisco Catalyst 2950, and the WLAN IP Telephony Manager 2245 connected with the Cisco Catalyst 2950.

Table 22
1230 connected with 2950 and 2245 connected with 2950

	AP: 1230	2950 connected the APs	2950 connected to 2245
1	class-map match-all class_SVP_VoIP match ip protocol 119 (protocol 119 marked the value of cos 5)	mls qos map cos-dscp 0 8 16 40 32 46 48 56	mls qos map cos-dscp 0 8 16 40 32 46 48 56
2	Policy-map wireles s-SVP-VoIP class class_SVP_VoIP	wrr-queue bandwidth 25 25 50 0 wrr-queue cos-map 1 0 1 2 4 wrr-queue cos-map 3 3 6 7 wrr-queue cos-map 4 5 (dscp 40 and 47 by default are marked as cos 5)	wrr-queue bandwidth 25 25 50 0 wrr-queue cos-map 1 0 1 2 4 wrr-queue cos-map 3 3 6 7 wrr-queue cos-map 4 5 (dscp 40 and 47 by default are marked as cos 5)

Copyright © 2004–2008 Nortel Networks

Table 22
1230 connected with 2950 and 2245 connected with 2950 (cont'd.)

	AP: 1230	2950 connected the APs	2950 connected to 2245
3	int fastethernet 0.240 encapsulation dot1Q 240 service-policy input wireless- SVP-VoIP	int fastethernet 026 (the port that is connected with the AP) switchport trunk native vlan 11 switchport trunk allowed vlan 11, 240 switchport mode trunk mls qos trust cos	int fastethernet 03 (the port that connected with 2245) switchport access vlan xx switchport mode access mls qos trust cos mls qos cos 5 service-policy input trust-voice-2 245
4	(for return path) dot11 priority-map avvid		class-map match-all voice-sig match access-group 100
5			access-list 100 permit udp 172.23.0.016 eq 5000 172.23.0.016
6			class-map match-all voice-bearer match access-group 101
7			access-list 101 permit udp 172.23.0.016 eq 5200 172.23.0.016
8			policy-map trust -voice-2245 class voice-sig set ip dscp 40 class voice-bearer set ip dscp 46

Table 23 "1230 connected with 3560 and 2245 connected with 6509" (page 175) provides the steps to configure the Cisco Aironet 1230 connected to the Cisco Catalyst 3560, and the Cisco Catalyst 6509 connected to the WLAN IP Telephony Manager 2245.

Table 23
1230 connected with 3560 and 2245 connected with 6509

	AP:1230	3650 connected to APs	6509 connected to 2245
1	class-map match-all class_SVP_VoIP match ip protocol 119 (protocol 119 marked the value of cos 5)	mls qos	mls qos
2	Policy-map wirele ss-SVP-VoIP class class_SVP_VoIP	mls qos map cos-dscp 0 8 16 40 34 46 48 56	mls qos map cos-dscp 0 8 16 40 32 46 48 56

Copyright © 2004–2008 Nortel Networks

Table 23
1230 connected with 3560 and 2245 connected with 6509 (cont'd.)

	AP:1230	3650 connected to APs	6509 connected to 2245
3	int fastethernet 0.240 encapsulation dot1Q 240 service-policy input wireless-SVPVoIP	interface fastethernet 01 priority-queue out mls qos trust cos	class-map match-all voice-sig match access-group 100
4	(for return path) dot11 priority-map avvid		access-list 100 permit udp 172.23.0.016 eq 5000 172.23.0.016
5			class-map match-all voice-bearer match access-group 101
6			access-list 101 permit udp 172.23.0.016 eq 5200 172.23.0.016
7			policy-map trust -voice-2245 class voice-sig set ip dscp 40 class voice-bearer set ip dscp 46
8			int fastethernet 03 (the port that is connected with 2245) switchport access vlan xx switchport mode access mls qos trust cos mls qos cos 5 service-policy input trust-voice-2 245

General WLAN configuration

The following is a list of considerations for general WLAN configuration:

- Multicast must be configured in any WLAN for Push-to-talk (PTT) on the WLAN Handset 2211.
- APs use channels 1, 6, and 11.
- APs require a 15-20dB separation for like channels to avoid cochannel interference.
- A one-way Performance domain is required (handset to call server): Max 100 ms delay, Max 30 ms jitter, and Max 2% packet loss.
- The WLAN IP Telephony Manager 2245 to AP link is (ideally) limited to 100 ms delay, 1 ms jitter and under 2% packet loss.

Copyright © 2004–2008 Nortel Networks

- The signal Strength must be -70dB or greater to provide sufficient voice quality and proper operation. Note that -60dB or better is required for 11 MB data rate.
- Wireless bridges are not permitted because they contribute to bottleneck delays.
- The transmission power must be the same on all APs and match the power setting on the handsets.
- AP bandwidth usage must be limited to 65 to 80% maximum for handset usage.
- The protocols used are: TCP, UDP, DHCP, DNS, WINS, TFTP, FTP, ARP, ICMP, and Telnet.
- The PTT feature uses the multicast IP address of 224.0.1.116 and is generally isolated to a single subnet.

DHCP server options

The DHCP server options known to work in almost every situation are 3, 7, 42, 66, 128, 151, and 152:

- DHCP Option 3—the Default Gateway
- DHCP Option 7—the Syslog Server
- DHCP Option 42—the Time Server
- DHCP Option 60—the Class Identifier
- DHCP Option 66—the IP address of the TFTP Server
- DHCP Option 151—the IP address of the WLAN IP Telephony Manager 2245
- DHCP Option 152—the IP address for the optional WLAN Application Gateway 2246

DHCP options have the same format as the BOOTP vendor extensions. Options can be fixed length or variable length. All options begin with a tag byte, which uniquely identifies the option. Fixed length options without data consist of only a tag byte. The value of the length byte does not include the tag and length fields.

Options containing NVT ASCII data (ideally) do not include a trailing NULL; however, the receiver of such options must be prepared to delete trailing NULLs if they exist. The receiver must not require that a trailing NULL be included in the data. With some variable-length options, the length field is a constant but it still must be specified.

Copyright © 2004–2008 Nortel Networks

DHCP options

This section provides the IEEE definitions of the DHCP options. The term SHOULD, as used in this section, is to be interpreted as described in [RFC2119].

DHCP option 1: Subnet Mask. Length: 6 bytes
This option specifies the client's subnet mask. If both the Subnet Mask and the router option are specified in a DHCP reply, this option MUST be first.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Mask

Code. 8 bits. Always set to 1.
Length. 8 bits. Always set to 4.
Mask. 32 bits. Subnet mask of the client.
RFCs: [RFC 2132] DHCP Options.
Updated by: RFC 3942.

DHCP option 3: Length: 6+ bytes This option specifies a list of 32 bit IP addresses for routers on the client's subnet. The routers SHOULD be listed in order of preference.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP address

Code. 8 bits. Always set to 3.
Length. 8 bits. 4+ in multiples of 4.
IP address. 32 bits. One or more IPv4 addresses.
RFCs: [RFC 2132] DHCP Options.
Updated by: RFC 3942.

DHCP option 6: 6+ bytes This option specifies a list of DNS servers available to the client. The servers SHOULD be listed in order of preference.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP address

Code. 8 bits. Always set to 6.
Length. 8 bits. 4+ in multiples of 4.
IP address. 32 bits. One or more IPv4 addresses.
RFCs: [RFC 2132] DHCP Options.

DHCP option 7: 6+ bytes This option specifies a list of MIT-LCS UDP servers available to the client. The servers SHOULD be listed in order of preference.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

Copyright © 2004–2008 Nortel Networks

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP address

Code. 8 bits. Always set to 7.
Length. 8 bits. 4+ in multiples of 4.
IP address. 32 bits. One or more IPv4 addresses.
RFCs: [RFC 2132] DHCP Options.
Updated by: RFC 3942.

DHCP option 15: 3+ bytes This option specifies the domain name that client should use when resolving hostnames via DNS.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Domain name

Code. 8 bits. Always set to 15.
Length. 8 bits. 1+.
Domain name. Variable length.
RFCs: [RFC 2132] DHCP Options

DHCP option 42: Length 4+bytes This option specifies a list of IP addresses indicating Network Time Protocol (NTP) servers available to the client. Servers SHOULD be listed in order of preference.

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
Code Length

16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP address

Code. 8 bits. Always set to 3.
Length. 8 bits. 4+ in multiples of 4.
IP address. 32 bits. One or more IPv4 addresses.
RFCs: [RFC 2132] DHCP Options.
Updated by: RFC 3942.

DHCP option 43 1+ Vendor specific information. RFC 1533, RFC 2132

DHCP option 60 1+ Class-identifier. RFC 1533, RFC 2132 – must be the string value of: Nortel-221x- A or Nortel-61xx-A

DHCP option 66 1+ TFTP server name. RFC 2132

DHCP option 128 TFPT Server IP address.

DHCP option 144 1+ Vendor specific information. RFC 1533, RFC 2132

DHCP option 151 1+ Vendor specific information. RFC 1533, RFC 2132

DHCP option 152 1+ Vendor specific information. RFC 1533, RFC 2132

DHCP option 157 1+ Vendor specific information. RFC 1533, RFC 2132

DHCP option 191 1+ Vendor specific information. RFC 1533, RFC 2132

Copyright © 2004–2008 Nortel Networks

DHCP support for handsets that emulate the IP Phone 2004

DHCP support in the IP Phone 2004 terminal requires a Class Identifier option with each DHCP Discovery and Request message. Additionally, the IP Phone 2004 checks for either a Vendor Specific option message with a specific, unique to Nortel IP Phone 2004 encapsulated subtype, or a site-specific DHCP option. In either case, a Nortel IP Phone 2004 specific option must be returned by the IP Phone 2004 aware DHCP server in all Offer and Ack messages. The IP Phone 2004 uses the information returned in this option to configure itself for proper operation. This configuration includes binding a new IP address, netmask and gateway (for the local IP stack) as well as configuring Server 1 (minimum) and, optionally Server 2. By default, Server 1 is always assumed to be the primary server after a DHCP session.

The IP Phone 2004 does not accept any Offers or Acks that do not contain all of the following options:

- a Router option
  The IP Phone 2004 requires a default router to function.
- a Subnet Mask option
- a Vendor Specific option
  OR
  a Site Specific option
  The initial DHCP implementation required only the Vendor Specific encapsulated suboption. In interop testing with WinNT (up to SR4), it was discovered that WinNT does not properly adhere to RFC 1541. As a result, it is not possible to use this option. The implementation was changed to add support for either Vendor Specific subops or Site Specific options. This new extension is tested and verified to work with WinNT.
  The site-specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for site specific use by the DHCP RFCs.

Format of the IP Phone 2004 Terminal DHCP Class Identifier field

All IP Phone 2004 terminals fill in the Class ID field of the DHCP Discovery and Request messages with Nortel-i2004-A:

- ASCII-encoded, NULL (0x00) terminated
- unique to Nortel IP Phone 2004
- –A uniquely identifies this version

Copyright © 2004–2008 Nortel Networks

Format of the IP Phone 2004 Terminal DHCP Encapsulated Vendor Specific option

The following definition describes the Nortel IP Phone 2004 specific, Encapsulated Vendor Specific option. This option must be encapsulated in a DHCP Vendor Specific option (Refer to RFC 1541 and RFC 1533) and returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone 2004 to accept these messages as valid. The IP Phone 2004 pulls the relevant information out of this option and uses it to configure the primary and (optionally) secondary TPSs. Either this encapsulated option or a similarly encoded site-specific option must be present. Configure the DHCP server to send one or the other—but not both. WinNT implementations must use the Site Specific option. For more information, see "DHCP support for handsets that emulate the IP Phone 2004" (page 180).

The format of the Encapsulated Vendor Specific option field is: Type, Length, Data.

- Type (1 octet): 5 choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251)
  With the choice of five types, the IP Phone 2004 can operate in environments where the initial choice is already in use by a different vendor. Select only one Type byte.
- Length (1 octet): variable—depends on message content
- Data (Length octets): ASCII-based—format Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr
  - Nortel-i2004-A uniquely identifies this as the Nortel option. Additionally, the -A signifies this version of this specification. For example, future enhancements could use -B.
  - ASCII (,)—separates the fields
  - ASCII (;)—separates the primary from secondary server info
  - ASCII (.)—signals the end of the structure
  - iii.jjj.kkk.lll:ppppp—identifies the IP:port for the server (ASCII-encoded decimal)
  - aaa—identifies the action for the server (ASCII-encoded decimal, range 0 to 255)
  - rrr—identifies the retry count for the server (ASCII-encoded decimal, range 0 to 255)

  This string can be NULL terminated although the NULL is not required for parsing.

Copyright © 2004–2008 Nortel Networks

Notes:

1. aaa and rrr are ASCII-encoded decimal numbers with a range of 0 to 255. They identify the Action Code and Retry Count, respectively, for the associated TPS server. Internally, to the IP Phone 2004, they are stored as one octet (0x00..0xFF). These fields must be no longer than three digits.
2. The first server is always considered the primary, and the second server always considered secondary.
3. If only one server is required, terminate the primary TPS sequence immediately with (.) instead of (;).
   Example: Norteli2004- A,iii.jjj.kkk.lll:ppppp,aaa,rrr
4. The valid options are one server or two servers (0, 3, or other numbers are not allowed).
5. The Action code values are:
   - 0 - reserved
   - 1 - UNIStim Hello (currently only this value is a valid choice)
   - 2 to 254 - reserved
   - 255 - reserved
6. iii,jjj,kkk,lll are ASCII-encoded, decimal numbers representing the IP address of the server. They need not be three digits long because the (.) and (:) delimiters guarantee parsing. For example, '001', '01', and '1' are all parsed correctly and interpreted as value 0x01 internal to the IP Phone 2004. These fields must be no longer than three digits each.
7. ppppp is the port number in ASCII-encoded decimal. It need not be five digits long because the (:) and (,) delimiters guarantee parsing. For example, '05001', '5001', '1', and '00001' are all parsed correctly and accepted as correct. The valid range is 0 to 65 535 (stored internally in the IP Phone 2004 as hexadecimal in the range 0 to 0xFFFF). This field must be no longer than five digits.
8. In all cases, the IP Phone 2004 treats the ASCII-encoded numbers as decimal values and ignores all leading zeros. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

Format of the IP Phone 2004 Terminal DHCP Site Specific option

The following definition describes the Nortel IP Phone specific, Site Specific option. This option uses the DHCP options 128 to 254 (reserved for site-specific use, see RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone 2004 to accept these messages as valid. The IP Phone 2004 pulls the relevant information out of this option and uses it to configure the primary and (optionally) secondary TPSs. Either this encapsulated

Copyright © 2004–2008 Nortel Networks

option or a similarly encoded site-specific option must be present. Configure the DHCP server to send one or the other—but not both. WinNT implementations must use the Site Specific option. For more information, see "DHCP support for handsets that emulate the IP Phone 2004" (page 180).

The format of the Terminal DHCP Site Specific option field is: Type, Length, Data.

- Type (1 octet): 5 choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251)
  With the choice of five types, the IP Phone 2004 can operate in environments where the initial choice is already in use by a different vendor. Select only one Type byte.
- Length (1 octet): variable—depends on message content
- Data (Length octets): ASCII-based—format Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr
  - Nortel-i2004-A uniquely identifies this as the Nortel option. Additionally, the -A signifies this version of this specification. For example, future enhancements could use -B.
  - ASCII (,)—separates the fields
  - ASCII (;)—separates the primary from secondary server information
  - ASCII (.)—signals the end of the structure
  - iii.jjj.kkk.lll:ppppp—identifies the IP:port for the server (ASCII-encoded decimal)
  - aaa—identifies the action for server (ASCII-encoded decimal, range 0 to 255)
  - rrr—identifies the retry count for the server (ASCII-encoded decimal, range 0 to 255)

  This string can be NULL terminated although the NULL is not required for parsing.

Notes:

1. aaa and rrr are ASCII-encoded decimal numbers with a range of 0 to 255. They identify the Action Code and Retry Count, respectively, for the associated TPS server. Internally, to the IP Phone 2004, they are stored as one octet (0x00..0xFF). These fields must be no longer than three digits.
2. The first server is always considered the primary, and the second server always considered secondary.

Copyright © 2004–2008 Nortel Networks

Notes:

3. If only one server is required, terminate the primary TPS sequence immediately with (.) instead of (;).
   Example: Norteli2004- A,iii.jjj.kkk.lll:ppppp,aaa,rrr
4. The valid options are one server or two servers (0, 3, or other numbers are not allowed).
5. The Action code values are:
   - 0 - reserved
   - 1 - UNIStim Hello (currently only this value is a valid choice)
   - 2 to 254 - reserved
   - 255 - reserved
6. iii,jjj,kkk,lll are ASCII-encoded, decimal numbers representing the IP address of the server. They need not be three digits long because the (.) and (:) delimiters guarantee parsing. For example, '001', '01', and '1' are all parsed correctly and interpreted as value 0x01 internal to the IP Phone 2004. These fields must be no longer than three digits each.
7. ppppp is the port number in ASCII-encoded decimal. It need not be five digits long because the (:) and (,) delimiters guarantee parsing. For example, '05001', '5001', '1', and '00001' are all parsed correctly and accepted as correct. The valid range is 0 to 65 535 (stored internally in the IP Phone 2004 as hexadecimal in the range 0 to 0xFFFF). This field must be no longer than five digits.
8. In all cases, the IP Phone 2004 treats the ASCII-encoded numbers as decimal values and ignores all leading zeros. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

Quality of Service checklist for voice over WLAN applications

The following QoS checklist pertains to voice over WLAN (VoWLAN) applications that use the WLAN Handset 2210/2211/2212.

1. For more information about SpectraLink Voice Priority (SVP) and why you need it, see the SpectraLink Voice Priority White Paper available from www.spectralink.com.

2. WLAN Access points must be SVP- or View-compatible as tested by SpectraLink Corp. Nortel requires all WLAN networks that carry voice be SVP-enabled or use WMM to receive NETS and GNTS support. For more information about SVP Compatible APs, go to www.spectralink.com.

Copyright © 2004–2008 Nortel Networks

3. Enable SVP in the APs. SVP must be enabled in all APs that carry voice traffic. Not all AP vendors use SVP terminology. Cisco 350,1100, and 1200 series APs, for instance, refer to SVP compatibility as Protocol 119 support. The SpectraLink Web site provides AP settings used in SVP compatibility testing. To download the AP configuration manuals, go to www.spectralink.com.

4. Configure the admissions limit in the 2245 Wireless IP telephony manager. The value you chose limits high-priority clients such as voice terminals from overloading an AP. The Nortel-recommended value is 7. An admissions limit higher than 7 can severely limit bandwidth to data users when voice traffic is high. To increase bandwidth for data, lower the admissions limit so that fewer voice terminals handover to the AP. WLAN performance studies with 802.11b radios show that the admissions limit must not exceed 10.

5. Handsets require a relative signal strength (RSSI) of -70dB or better for high QoS. When the RSSI drops below -70dB, handsets attempt to handover to an AP with a higher RSSI.

6. Up to three APs can occupy the same area because 802.11b provides three nonoverlapping channels. Handsets require like-channels, between adjacent APs, to have 15-20dB of separation to achieve good QoS and to avoid ping-pong between APs, which impacts QoS by creating constant handover.

7. WLAN infrastructure must be configured for high performance with delay between 221x handset and 2245 less than 100 ms, less than 1% packet loss and less than 30 ms jitter. WLAN networks that previously only supported data applications sometimes cannot meet this performance criteria and consequently are not be suitable for voice services.

8. RF cochannel interference reduces both the capacity and reach of WLAN networks. Use site surveys to plan coverage areas and scan them to insure that Rogue APs are not present. Cochannel interference can also be created by florescent light, microwave ovens, 2.4 GHz analog or digital telephones, Bluetooth adapters, and 2.4 GHz frequency-hopping applications such as first generation AP or DECT 2.4 GHz wireless.

9. Building construction can impact RF. Metal floors, metal walls, and metal ceilings can create RF signal reflections, and create a scenario known as multipath, which creates interference to the voice packet stream.

10. Handsets have a built-in Site Survey mode that shows the actual RSSI from the four strongest APs at any current location. Use Site Survey mode to determine holes in coverage that can create dropped calls or poor voice QoS.

11. Poor voice QoS received in handsets is caused, 70% of the time, by problems in the infrastructure, such as missing SVP enabled, poor RSSI coverage, cochannel interference, Ethernet duplex mismatch, excessive retransmission of packets, or other RF interference.

Copyright © 2004–2008 Nortel Networks

RF basics and AP configuration

The following points include the characteristics of a good RF environment that uses access point parameters for Nortel wireless telephone voice communications. Only channels 1, 6, and 11 are used.

- Disable auto-channel select features and use fixed channels.
- Fix the transmit (TX) power setting and disable auto-power features.
- Ensure that access points have a consistent and same power setting, unless there is a compelling reason to deviate
- Configure areas where wireless telephone users can congregate with special care:
  - Position APs closer together to provide greater bandwidth for an area.
  - Turn down the AP TX power.

  It is a very complicated process to accomplish this task properly.
- Configure the wireless telephone transmit power levels to match the standard for the RF environment.
  Consider the antenna gain used on the access points when adjusting the wireless telephone power setting.
- Ensure that there is -70dBm RF signaling or better available in all areas designated for wireless telephone operation.
  For this signaling requirement, all four 802.11b data rates must be available to the wireless telephones. The four 802.11b data rates are: 1Mb/s, 2Mb/s, 5.5Mb/s, and 11Mb/s.
  The best configuration is for all four to be configured to Basic or Required. For manufacturer-specific settings, see the guidelines from SpectraLink. Define this parameter, as Basic or Required, in the AP and configure the following:
  - 802.11g data rates can be configured to Enabled.
  - Multicast packets use only 802.11b data rates configured to Basic or Required.
  - If 802.11 wireless devices are used, 5.5Mb/s and 11Mb/s can require the parameter be configured to Enabled or Supported, rather than Basic.
    Ensure that there is a compelling reason to do so, before you make this change.
- Configure the Beacon interval to 100 ms and DTIM to 3.
- Use appropriate security mechanisms for the wireless telephones and the requirements of the environment:

Copyright © 2004–2008 Nortel Networks

— Nortel WLAN IP Telephony telephones support WEP, WPA-PSK, or WPA2-PSK.

— Nortel recommends that you always use Open Authentication because it is more secure.

— You can use a No WEP temporary SSID during troubleshooting so that you can gather wireless data with visibility into the SpectraLink Radio Protocol (SRP) data structures.
After troubleshooting is complete, disable this temporary SSID.

- Ensure 15% to 20% cell overlap between AP signal coverage areas.
- Always use two antennas on each AP.

  — Enable diversity in each AP.

  — Use full diversity in each AP, not partial or one-way diversity.

  — Make this the standard for the RF environment.
  Very special circumstances must exist before you make changes.
- Provide priority for IP protocol 119 packets:

  — Assign voice packets to an AP QoS Class of Service with a latency of 10 ms or less.

  — Configure priority for both directions in both interfaces.
  Priority gets the voice packets ahead of the queue inside the AP, whether the interface is 802.11b radio or Ethernet.

  — Configure Voice Radio Contention Window Minimum to 0.

  — Configure Voice Radio Contention Window Maximum to 0.

  — Configure Voice Fixed Slot Size to 2.

  — Configure Voice Transmit Opportunity to 0.

  On the Cisco Aironet 1200 Series with code 12.3(8)JA3 or later, click WFA Default on QoS Radio 802.11g. Access the Categories page and then configure the parameters for voice. This version has two boxes to configure for each parameter. Do not click Optimize for Voice.
- Enable WiFi Multi-Media (WMM) on the radio interface.
- Use VLAN support in the AP and in the network for security and management:

  — Assign the voice SSID to a VLAN.

  — Enable the voice VLAN across the network between the AP, to the SVP, to the Signaling Server, to the Call Manager and all components in between.

  — Assign all devices in this VLAN to one subnet.

Copyright © 2004–2008 Nortel Networks

  - Ideally, there is no routing between any network devices used for voice communication.
  - If routing is necessary, keep it in the back-end, between the SVP and PBX Call Server. Keep routing short and quick.

There are other access point parameters necessary for the proper operation of voice communications. Often, these are not adjustable. By specifying IP protocol 119 the following parameters are enabled on the voice path in the access point:

- Voice packet retry limit of three
  If a voice packet is not ACKed, it is retried three times and then dropped. This parameter must be enabled in the code to be able to control the number of packet retries and limit them to three. There are access points that identify IP protocol 119 (SpectraLink voice packets), to limit packet retries to three and other access points simply identify voice transmissions to limit retries.
- Round Robin Queuing
  During voice packet retry transmissions, the AP can also transmit other voice packets in the queue. This ability prevents other wireless telephones that use the AP from having their voice communications held up while retries occur. This causes all other wireless telephones to have poor audio while one wireless telephone is in a retry state.

These parameters can be invoked by specifying the voice profile or IP protocol 119 < 10 ms latency. Disable the following parameters:

- Dynamic Transmit Power at the Control (DTPC) for wireless clients
- AP Dynamic TX Power (or configure to On Demand Only)
- AP Dynamic Channel Select (or configure to On Demand Only)
- Intrusion Detection System (IDS) involvement
  IDS causes the AP to go off channel and listen for other wireless clients and APs. This causes degraded voice quality.
- Load balancing at the AP for clients and network
- Interference detection and avoidance
- Coverage hole detection and correction
- Client Holdoff Time
- EAP or MAC Reauthentication interval
- TKIP MIC Failure Holdoff Time

Copyright © 2004–2008 Nortel Networks

Troubleshooting

Ensure that the WLAN IP Telephony and PBX product mix lines up with the compatibility matrix in the current Product Bulletin.

If the site does not conform, it is not classified as a supported installation.

Diagnosis flows

The following sections provide information about the troubleshooting process for different types of issues.

Call or signalling-related issues

Signaling issues are not normally a result of an issue with the IP data network. However, if an IP data network is congested or configured incorrectly, signaling traffic can be affected. Because call signaling is normally a combination of H.323 (TCP)- and Reliable User Datagram Protocol (RUDP) (IP Sets)-based traffic, the packets usually reach the destination, barring any IP network configuration issues. However, these packets could drop and cause excessive retransmission and delay. As an example, the IP phones keep-alive communication with the signaling server can be affected.

Table 24
Typical call-related issues

Issue	Type of issue	Check for
Unable to place a call	Network	IP phone: IP connectivity to Signaling server IP connectivity issues to other IP sets Excessive congestion or retransmissions Analog or digital phone: IP trunk connectivity issues
	Product	IP, analog, or digital phone: Phone configuration Dial plan
IP phone resetting	Network	IP connectivity to Signaling server Network congestion
	Product	Incorrect phone configuration
Call disconnects or drops during a conversation	Network	Intermittent network congestion that affects the keep-alive
	Product	Signaling issues Incorrect configuration

Copyright © 2004–2008 Nortel Networks

Voice-quality issues

The transport, or IP data network, are the most likely causes of voice-quality issues. In some circumstances, product issues (such as echo or Digital Signal Processor (DSP) errors) can cause problems with voice quality. The data network does not introduce echo into a conversation, but it can enhance existing echo.

In a converged environment, voice competes with data traffic for bandwidth and processor time. As a result, the IP data network must be optimized for efficient processing of the real-time voice packets.

Table 25
Typical voice quality issues

Issue	Type of issue	Check for
Choppy voice	Network (usually)	Network delay caused by: Excessive intermittent end-to-end round-trip delay Congestion Queuing Network configuration errors
		Packet loss caused by: Physical errors in data network Network configuration errors
First or last part of word syllables missing	Product (usually)	Incorrect Voice Activity Detection (VAD) configuration OR Incorrect AP configuration (if the issue occurs only during roaming)
Clicks or pops heard during conversation		Packet loss, cause depends on the codec
One-way speech path	Network	IP routing issues Congestion issues
	Product	Incorrect configuration
Voice delay (users talk over each other)	Network	Excessive network delay
Echo	Network	Data network can enhance echo
	Product (primarily)	

Copyright © 2004–2008 Nortel Networks

Handset error messages

Table 26 "Handset error messages" (page 191) shows error messages that appear on the liquid crystal diode (LCD) display of the wireless handsets.

Table 26
Handset error messages

Short	Error code	Description	Action
Assert	Assert Errors	The phone detects possible network errors and cannot recover without configuration modification.	Verify the AP settings: data rates and fragmentation threshold. Use the Configuration Cradle to capture the assert error and then send the error to Nortel GNTS.
Code	Bad Code Type	The license management setting on phone is incorrect.	Adjust the license management setting.
DHCP	DHCP Error(s)	A problem communicating with DHCP server exists.	Troubleshoot the DHCP server configuration and the network.
DHCP	Can’t Renew DHCP	The DHCP server is not responding to a lease-renewal attempt.	Troubleshoot the DHCP server configuration and the network.
Duplicate	Duplicate ID	Two phones are configured with the same IP address.	Configure a valid static IP address for the phone. Check the DHCP configuration.
ESSID	Bad ESSID	The ESSID on the phone does not match the SSID on the AP.	Configure the correct ESSID statically on the phone.
Flash Config	Flash Config Error	The internal configuration of the phone is corrupt.	Restore the phone defaults and enter the configuration information.
No Net	No Net Found	The ESSID on the phone does not match the SSID on the AP.	Configure the correct ESSID statically on the phone.
No Net	No Net Access	The security settings on the phone do not match the security settings on the AP.	Check the AP security settings and configure the security settings for the phone to match.

Copyright © 2004–2008 Nortel Networks

Table 26
Handset error messages (cont'd.)

Short	Error code	Description	Action
PBX	No PBX	The phone is not communicating with the PBX.	Check the cross connects, bridge clips, punch downs on demarcation block, amphenol tail. and PBX (see if the extension is built correctly).
SVP	No SVP Response	The phone cannot communicate with the WLAN IP Telephony Manager 2245.	Configure the Ethernet switch port and SVP to 100/full. Forward the DHCP option 151 to the IP of the SVP server. Verify the settings on the AP. Verify that there is no 2.4 Ghz interference of any kind.
SVP	No SVP IP	No static IP entered into the phone for the WLAN IP Telephony Manager 2245.	Check for a valid IP in the phone. Check the license management configuration. Compare a working phone code to the nonworking phone code.
SW	No SW Found	No phone code is found on the TFTP server.	Point the TFTP software to the correct directory that contains valid code.
System	System Locked	The WLAN IP Telephony Manager 2245 is locked.	Dial in and verify that system is locked. Soft reset the SpectraLink infrastructure through the menu system.
TFTP	TFTP Error(s)	A failure occurred during the TFTP software update.	Check the TFTP software (SolarWinds is not compatible). Check the TFTP configuration. Forward option 66 in the DHCP scope, to the IP address of the TFTP server.

Timing information

The WLAN IP Telephony Manager 2245 sends payload packets to the handset every 30 ms in a 5 ms window. The handsets are likely to experience issues if the jitter between the WLAN IP Telephony Manager 2245 and the AP is greater than 5 ms. Ideally, jitter in this part of the network is 1 ms or less.

Copyright © 2004–2008 Nortel Networks

Table 27
Timing

WLAN IP Telephony Manager 2245 to the AP	Handset to the WLAN IP Telephony Manager 2245
Delay ≤ 100 ms	Delay ≤ 100 ms
Jitter ≤ 1 ms	Jitter ≤ 30 ms
Packet loss ≤ 2%	Packet loss ≤ 2%

The handset sends a handshake to the WLAN IP Telephony Manager 2245 every 30 seconds. If no response is received from the WLAN IP Telephony Manager 2245, the handset tries four more times, for a total of five attempts. If none of these get a response from the WLAN IP Telephony Manager 2245, the handset attempts to find a different AP and repeats the above handshake sequence. If the handset cannot find another AP or the second attempt fails, the No SVP Response message appears on the handset LCD display.

Diagnostic Tools

Run Site Survey, Diagnostics Mode, and Syslog Mode are provided to assist the WLAN administrator to evaluate the functioning of the handset and the VoWLAN system. These tools are enabled from the handset Admin menu.

Run Site Survey for the WLAN Handset 2210/2211/2212

Site Survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs, regardless of ESSID. The information available through Site Survey includes:

- ESSID
- beacon interval
- information regarding support of various protocols and standards, as required
- current security configuration

When Run Site Survey begins, it is in single ESSID mode. Press the **Any** soft key to switch to all APs (regardless of ESSID) mode; the **Any** soft key changes to **MyID**. The display looks like the following in multiple AP mode:

Copyright © 2004–2008 Nortel Networks

```
111111 -22 33       444

111111 -22 33       444

111111 -22 33       444

111111 -22 33       444

MyID                Detl
```

where

111111 = last three octets of the ESSID for the discovered AP
22 = signal strength of the specified AP
33 = channel number of the specified AP
4444 = DTIM interval configured for the specified AP
MyID = soft key to toggle between single and any ESSID mode
Detl = soft key to toggle between summary and detail screens

Press the **Detl** soft key to view the details, as follows:

```
i:bbbbb sn ch bcn

eeeeeeeeeee DGHI

rrrrrrrrrrrrr+xxxx

mmm G:gggg P:pppp
Any                     Smry
```

where

i = index of selected AP (range: 0-3)
bbbbb = last three octets of the ESSID for a discovered AP
sn = signal strength in -dBm
ch = channel
bcn = beacon interval
eeeeeeeeeee = ESSID (up to first 11 characters)
DGHI = standards supported
rrrrr = rates supported (example: 1b2b5b11b)
+ = more rates supported than displayed
xxxx = WMM or UPSD if supported
mmmm = security mode
G:gggg = group key security

Copyright © 2004–2008 Nortel Networks

P:pppp = pair-wise key security
Any = soft key to toggle between single and multiple ESSID mode
Smry = soft key to return to summary display

Run Site Survey for the WLAN Handset 6120/6140

Site Survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs, regardless of SSID. The information available through Site Survey includes:

- SSID
- beacon interval
- information regarding support of various protocols and standards, as required
- current security configuration

When Run Site Survey begins, it is in single SSID mode. Press the Any soft key to switch to all APs (regardless of SSID) mode; the Any soft key changes to MyID. The display looks like the following in multiple AP mode:

111111 -22 33	444
111111 -22 33	444
111111 -22 33	444
111111 -22 33	444
MyID	Detl

where

111111 = last three octets of the SSID for the discovered AP
22 = signal strength of the specified AP
33 = channel number of the specified AP
4444 = DTIM interval configured for the specified AP
MyID = soft key to toggle between single and any SSID mode
Detl = soft key to toggle between summary and detail screens

The following display shows three APs configured with an SSID that matches that of the handset. The first has a signal strength of –28dBm, and is configured on channel 2 with a beacon interval of 100 ms. The

Copyright © 2004–2008 Nortel Networks

second has a signal strength of –48dBm, and is configured on channel 6 with a beacon interval of 200 ms. The third has a signal strength of –56dBm and is configured on channel 11 with a beacon interval of 100 ms.

ab7bc8 -28 02	100
2ae578 -48 06	200
2ae596 -56 11	100
Any	Detl

When you select Any SSID mode, the summary display contains the first six characters of the APs SSID instead of the beacon interval, as shown in the following example.

ab7b -28 02	ALPHA
2ae5 -48 06	WSMTES
2ae5 -56 11	voice
Any	Detl

In detail mode, the display appears as follows. The left and right arrow keys move between AP indices.

```
i:bbbbb sn ch bcn

eeeeeeeeeee DGHI

rrrrrrrrrrrrr+xxxx

mmm G:gggg P:pppp
Any                        Smry
```

where

i = index of selected AP (value is from 0 to 3 inclusive)
bbbbb = last three octets of the SSID for a discovered AP
sn = signal strength in -dBm
ch = channel
bcn = beacon interval
eeeeeeeeeee = SSID (up to first 11 characters)
DGHI = standards supported

Copyright © 2004–2008 Nortel Networks

rrrrr = rates supported—basic rates have a b following the rate
+ = more rates supported than displayed
xxxx = WMM or UPSD if supported
mmmm = security mode
G:gggg = group key security
P:pppp = pair-wise key security
Any/MyID = soft key to toggle between single and multiple SSID mode
Detl/Smry = soft key to toggle between the multiple AP display (summary) and the single AP display (detail)

ATTENTION
Numbers racing across the handset display indicate that AP information is being obtained. A Waiting message indicates that the system is not configured properly and the handset cannot find any APs.

Diagnostics Mode

Diagnostics Mode evaluates the overall quality of the link between the handsets, AP, and the infrastructure equipment (call server, WLAN IP Telephony Manager 2245, and gateways). Diagnostics Mode can be used when the handset is active.

When Diagnostics Mode is activated in the Admin menu, the handset enters the diagnostic state. The handset can display diagnostics any time it is on a call.

Pressing the **Menu** key displays a number of diagnostic counters. Five screens of counters can be displayed by pressing the **Menu** key to scroll through the following screens:

- Screen 1—displays counters for missed receive packets, missed transmit packets, receive retry count, and transmit retry count.
- Screen 2—displays jitter delta, last successful transmit data rate, and gateway type.
- Screen 3—displays a list of APs and some of their details.
- Screen 4—displays association and reassociation counts.
- Screen 5—displays security error count and sequence number for last security error.

After all the counters are displayed, the screen returns to the normal off-hook display.

The screen number appears on the top line of the screen.

Copyright © 2004–2008 Nortel Networks

Diagnostics Screen 1 displays the following information:

MissedRcvCnt	nnnnn
MissedXmtCnt	nnnnn
RxRetryCount	nnnnn
TxRetryCount	nnnnn

where

MissedRcvCnt is the missed receive packet count since power up.
MissedXmtCnt is the missed transmit packet count since power up.
RxRetryCount is the receive retry count since power up.
TxRetryCount is the transmit retry count since power up.

Diagnostics Screen 2 displays the following information:

Jitter	nnnnn
LastRate	nnnnn
GatewayType	mnemo

where

Jitter is the current delta from the desired jitter buffer depth, in microseconds.
LastRate is the last successful transmit data rate.
GatewayType is a mnemonic that indicates the gateway type. The mnemonic is one of:

SAWA2	all phones are rate limited to 2 Mb because an old 2 Mb handset is on the network (not applicable for the WLAN Handset 6120 and the WLAN Handset 6140)
2Mb	old style 2 Mb (not applicable for the WLAN Handset 6120 and the WLAN Handset 6140)
11Mb	New style 11 Mb (for all handsets)

Diagnostics Screen 3 displays a list of the APs that are heard, in the following format:

C : mmmm ch - ss	aid
1 : mmmm ch - ss	mnem

Copyright © 2004–2008 Nortel Networks

2 : mmmm ch - ss	mnem
3 : mmmm ch - ss	mnem

where

C is the AP currently in use.
1, 2, and 3 are the candidate APs.
mmmm is the hexadecimal number comprised of the last two octets of the AP MAC address.
ch is the channel number that the AP is configured on.
ss is the signal strength for the AP in dBm.
aid is the Association ID of the currently associated AP.
mnem is a mnemonic that indicates why the handset did not hand off to this candidate:

Unkn	reason unknown
Weak	signal strength too weak
Rate	One or more basic rates not supported
Full	AP cannot handle bandwidth requirements
AthT	Authentication Timeout
AthF	Authentication Failure
AscT	Association Timeout
AscF	Association Failure
SecT	Security Timeout
SecF	Security Failure
Cnfg	Configuration error—AP is not configured correctly (check security, QoS mode, or network infrastructure)

Diagnostics Screen 4 displays the following information:

AssocCount	nnnnn
ReAssocCount	nnnnn
AsssocFailure	nnnnn
ReAssocFail	nnnnn

where

AssocCount is the association count since power up.
ReAssocCount is the reassociation count since power up.
AssocFailure is the number of association failures since power up.
ReAssocFail is the number of reassociation failures since power up.

Copyright © 2004–2008 Nortel Networks

Diagnostics Screen 5 displays the following information:

Sec-ErrCount	nnnnn
LstSecErrSeq	nnnnn

where

Sec-ErrCount is the security error count since power up.

LstSecErrSeq is the MAC frame sequence number with the last security error.

Syslog Mode

A Syslog Server must be present on the network so that the handset can send log messages and have them saved. The Syslog Server IP address can be configured using DHCP or statically configured.

ATTENTION
If the Syslog Server address is blank (000.000.000.000 or 255.255.255.255) or the handset is using DHCP and no option 7 is received from the DHCP server, the handset does not send any syslog messages.

Each syslog message includes the following:

- Date and time (to 1100th of a second) since the handset power on (configured to January 1 00:0:00); requires an SNTP server
- WLAN Handset MAC address
- WLAN Handset IP address
- Sequence number
- plus, additional items, based on the message type, as shown in Table 28 "Syslog message contents" (page 201).

Message example:

```
Jan 1 00:01:26 0090.7a02.2a1b (172.16.0.46) [001a] RStat: AP
00:40:96:48:1D:0C (-56dBm), Sent 783523, Recvd 791342, MSnt 245, MRcd
5674, BSnt 43, BRcd 10783, TX drop 43 (0.0%), TX retry 578 (1.2%), RX retry
1217 (1.6%).
```

Table 28 "Syslog message contents" (page 201) contains the contents of the syslog messages.

Copyright © 2004–2008 Nortel Networks

Table 28
Syslog message contents

Syslog message	Contents
Failed Handoff (sent whenever the handset decided to hand off, but failed trying)	Failed AP MAC Failed AP signal strength Current AP MAC Current AP signal strength Failure reason
Successful Handoff	New AP MAC New AP signal strength Old AP MAC Old AP signal strength Reason for handoff Other candidate APS: • MAC • Signal strength • Reason not used
Security Error	AP MAC AP signal strength Security mode Error details (mode dependent)
Call Start	Call type (telephony, OAI, PTT) AP MAC AP signal strength
Call End	AP MAC AP signal strength

Copyright © 2004–2008 Nortel Networks

Table 28
Syslog message contents (cont'd.)

Syslog message	Contents
Audio stats (AStat)	AP MAC AP signal strength Payload size (in ms) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter
Audio threshold (AThresh) exceeded (Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 ms)	AP MAC AP signal strength Payload size (in ms) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter

Copyright © 2004–2008 Nortel Networks

Table 28
Syslog message contents (cont'd.)

Syslog message	Contents
Radio stats (NStat)	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)
Radio threshold (NThresh) exceeded (Sent if TX drop rate exceeds 2%, or TX or RX retry rate exceeds 5%)	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received

Copyright © 2004–2008 Nortel Networks

Table 28
Syslog message contents (cont'd.)

Syslog message	Contents
	TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)
VPN: Established IKE phase 1 SA, renew in xs VPN: Established IKE phase2 SA yy:yy, renew in xs (a phase1 message follows the phase 2 message, sent whenever a phase 1 or phase 2 security association completes)	Expiration time and security association identifiers, if applicable. xs is the number of seconds yy:yy stands for the two eight-digit SA numbers for send and receive
VPN: phase2 Unexpected message VPN: phase2 Initiated by VN server VPN: phase2 INFO Delete payload	none

Table 29
Syslog reason codes

Reason code number	Meaning
0	OK
1	TOO FEW AVERAGE PROBES
2	WORSE SIGNAL
3	INVALID SSID
4	NO PARAMS FOUND
5	BAD RATES
6	OFF CHANNEL PROBE RESP
7	AP TOO BUSY
8	AUTH TIMEOUT
9	ASSOC TIMEOUT
10	FAILED AUTHENTICATION

Copyright © 2004–2008 Nortel Networks

Table 29
Syslog reason codes (cont'd.)

Reason code number	Meaning
11	FAILED ASSOCIATION
12	SOFT NEIGHBOR
13	NO SIG IMPROVEMENT
16	NO KEEPALIVE
17	LOST AUDIO
18	NO RESPONSE
19	NO PRIVACY
20	APP UNHAPPY
21	DISASSOCIATED
22	NO HANDOFF
23	HANDOFF
24	INITIAL ASSOC
25	LOST AP
26	TX FAILURES
27	CHANGING RATES
28	UNDEFINED
29	EAP START TIMEOUT
30	LEAP CHALLENGE TIMEOUT
31	EAP SUCCESS TIMEOUT
32	LEAP CHALLENGE RESPONSE TIMEOUT
33	NONCE CCKM TIMEOUT
34	RSNIE AP TIMEOUT
35	NONCE GTK TIMEOUT
36	EAPOL LOGOFF
37	EAPOL FAILURE
38	NO WPA ELEMENT
39	BAD MIC
40	BAD PROBE RESP
41	BAD CAP INFO AD HOC
42	ACTION TIMEOUT
43	FAILED ACTION

Copyright © 2004–2008 Nortel Networks

Table 29
Syslog reason codes (cont'd.)

Reason code number	Meaning
44	DELTS
45	QOS REQUIRED
46	CHANGED LISTEN INTERVAL

Data capture

Use the information presented in this section to begin capturing the correct data for analysis.

Questions

Ask the following questions to help isolate the source of a problem:

- Is the issue present with handsets that are associated to the same AP—yes or no?
- Is the issue present with handsets that are associated to different APs, which are associated to same controller—yes or no?
- Is the issue present with handsets that are associated to different APs, which are associated to two different controllers in the same mobility group—yes or no?

Data checklist

Gather the following data from the site for analysis:

- wired ip sniffer trace on the mirrored port for the WLAN IP Telephony Manager 2245
- wireless ip sniffer trace at the AP to which the test handset is associated
- syslog capture
  For more information, see "Syslog capture configuration" (page 208).
- logs of the event from the Signaling Server
- isetShow output from the Signaling Server or from the Voice Gateway Media Card (VGMC) running as Leader
- screenshots of each screen in the WLAN IP Telephony Manager 2245
- screenshots of the DHCP server scope with the fields fully expanded (no truncation of data in the view)

Copyright © 2004–2008 Nortel Networks

Figure 34
DHCP scope

Option	Name	Vendor	Value	Class
003	Router	Standard	10.25.8.1	None
060	Class Identifier	Standard	Nortel-221x-A	None
066	TFTP Server	Standard	10.25.8.10	None
128	Nortel i2004	Standard	Nortel-i2004-A,172.25.11.11:4100,1.7.	None
151	2245 WLAN TM Master	Standard	10.25.8.11	None
152	2246 WLAN AG	Standard	10.28.8.21	None

Notes:

1. Before you begin the data capture, disable any encryption protocols so that the data can be analyzed. If this is not possible, you must supply the encryption keys.
2. Time sync the wired and wireless IP sniffer traces (to the second if possible) and note whatever difference is present. This is crucial for the captures to be analyzed as a whole event.
3. Include the Nortel case number and the capture date in the name of each file.
4. Use a compression program to compress the files before you send them. If the files are password protected, send the passwords in a separate e-mail.

ATTENTION
VERY IMPORTANT
All captures, except the screenshots, must be concurrent during the same time frame that the problem scenario is executed. This ensures that each capture is for the same problem scenario.

Site-data required for the capture analysis

To analyze the captured data, certain site information is required. Ensure that the information is current for the time at which you obtain the captures. Gather the following information for your site:

- the MAC address of the test handset
- the alias IP of the test handset
- the DHCP supplied IP or manually configured static IP of the test handset
- the IP and MAC addresses of the WLAN IP Telephony Manager 2245
- the TLAN and ELAN IPs for the Signaling Servers

Copyright © 2004–2008 Nortel Networks

- the TLAN and ELAN IPs for the Voice Gateway Media Cards (VGMC)
- a network diagram
  For more information, see “Network diagram” (page 208).
- a site survey
- screenshots of the DHCP server scope with the fields fully expanded (no truncation of data in the view)
- the encryption protocol
- the software version of the WLAN IP Telephony Manager 2245
- the firmware version of the test handset
- the release (RLS) of the PBX software
- the version of the code that currently runs on the Signaling Servers
- the software version on the VGMCs
- the make, model and software version of the AP, the Controller or the WLAN Manager

Network diagram

For each element in the network, include the following information as it applies to each element:

- manufacturer
- model identification
- software version
- firmware version
- loadware version
- IP addresses
- MAC addresses
- port assignments
- VLANs
- other connectivity information

Syslog capture configuration

Configure DHCP Option 7 with the IP of the Syslog Server or, if you are not using DHCP, configure this manually as a static entry in the handset

Configure the IP of the Syslog Server in the WLAN IP Telephony Manager 2245: Network configuration > Syslog Server.

Copyright © 2004–2008 Nortel Networks

Configure the handset:

- Admin Menu > Diagnostics > Diagnostics mode on
- Admin Menu > Diagnostics > Syslog mode > full

If a Syslog Server is not available, use a public domain Syslog—for more information, see the KIWI Syslog Daemon available from www.kiwisyslog.com.

Signaling Server log capture

Use the CLI to obtain a log capture from the Signaling Server.

Procedure 28
Using the CLI to capture a Signaling Server log

Step	Action
1	Open a telnet session to the Signaling Server.
2	Start a file capture of the telnet session.
3	Use the level 2 pdt password for the system to enter pdt.
4	Change to the directory where the logs are stored. For more information, see the appropriate system documentation.
5	Determine the date stamps of the log files that cover the time frame for the problem scenario: `ll`
6	For a log file, run the command: `rdopen log000xx.rpt` The response from the SS is Reading log000xx.rpt.
7	For the same log file, run the command: `rdall`
8	Repeat Step 6 and Step 7 for each log file.
9	End the telnet file capture.
10	Zip the capture and send it to Nortel.
	--End--

General data capture

Before you run the show run-config or debug commands, enable text capturing on your Hyper terminal or Telnet application that you use to access the WLAN Security Switch 2270.

Copyright © 2004–2008 Nortel Networks

Multiple times is better—copy and paste the following commands on the WLAN Security Switch 2270 CLI, rather than typing them individually. The screen begins scrolling with output as soon as you type the commands.

- show run-config (from all WLAN Security Switch 2270s)
- show tech support
- show msglog

The wired sniffer must sniff the Gig port of the WLAN Security Switch 2270. No capture filter is required; get everything.

Obtain the wireless capture from the channel that the handsets currently use. Configure the wireless sniffer to capture from only one channel. To determine which channel, first show the client summary. Look for the MAC of the client showing status associated and note the name of the AP beside it. To see the channel that the AP operates on, show the advanced 802.11b summary.

Follow the steps in Procedure 29 “Obtaining the wired and wireless captures” (page 210), to capture data to send to Nortel for analysis.

Procedure 29
Obtaining the wired and wireless captures

Step	Action
1	Run the command: **`debug airwave-director all enable`** Let this command run for 5 to 7 minutes.
2	Run the command: **`debug disable-all`**
3	Run the following debug commands from the WLAN Security Switch 2270 (that you are testing) in the CLI: **`debug dot11 mobile enable`** **`debug dot11 state enable`** **`debug mobility directory enable`** **`debug mobility handoff enable`** **`debug pem state enable`** **`debug pem events enable`** **`show debug`**
4	Start the wireless and wired sniffer captures.
5	Initiate a handset to handset regular call or Push-to-talk call.
6	Continue the voice conversation for 1 to 2 minutes.
7	End the call that you established in Step 5.

Copyright © 2004–2008 Nortel Networks

8 End debug; copy and paste the following commands on the CLI:

```
debug disable-all
show debug
```

9 Stop the wired and wireless captures.

10 Zip the captures and send them to Nortel.

--End--

Scan for interference. MetaGeek Wi-Spy 2.4GHz Spectrum Analyzer is one low-cost option. For more information, go to www.metageek.net.

Capture assert error messages with the Configuration Cradle

One of the key features of the Configuration Cradle is the ability to extract assert error data when the handset (WLAN Handset 2210/2211/2212) encounters an exception condition and cannot recover from it gracefully. This dump contains information with which the design team can quickly isolate and fix the problem.

The Assert Error message appears on the LCD display after the handset detects a system error from which it cannot recover. The assert error data is stored in flash memory until you power cycle the handset. You can use the Configuration Cradle to retrieve this information as an .asrt file, which you can then send to Nortel technical support for further debugging.

Use the steps in Procedure 30 “Recording an assert error message” (page 211) to record and retrieve assert error data.

ATTENTION
Do not replace the battery pack before you perform the steps in Procedure 30 “Recording an assert error message” (page 211).

Procedure 30
Recording an assert error message

Step	Action
1	Write down the error message that appears on the LCD display.
2	While the Config program is running, remove the battery pack and place the handset in the Configuration Cradle.
3	Open the **File** menu and select **Get Assert Information**.
4	Browse to the location to which you want to save the .asrt file.
5	Click **Get Assert Data.** The handset uploads the .asrt file to the location that you specified in Step 4.

Copyright © 2004–2008 Nortel Networks

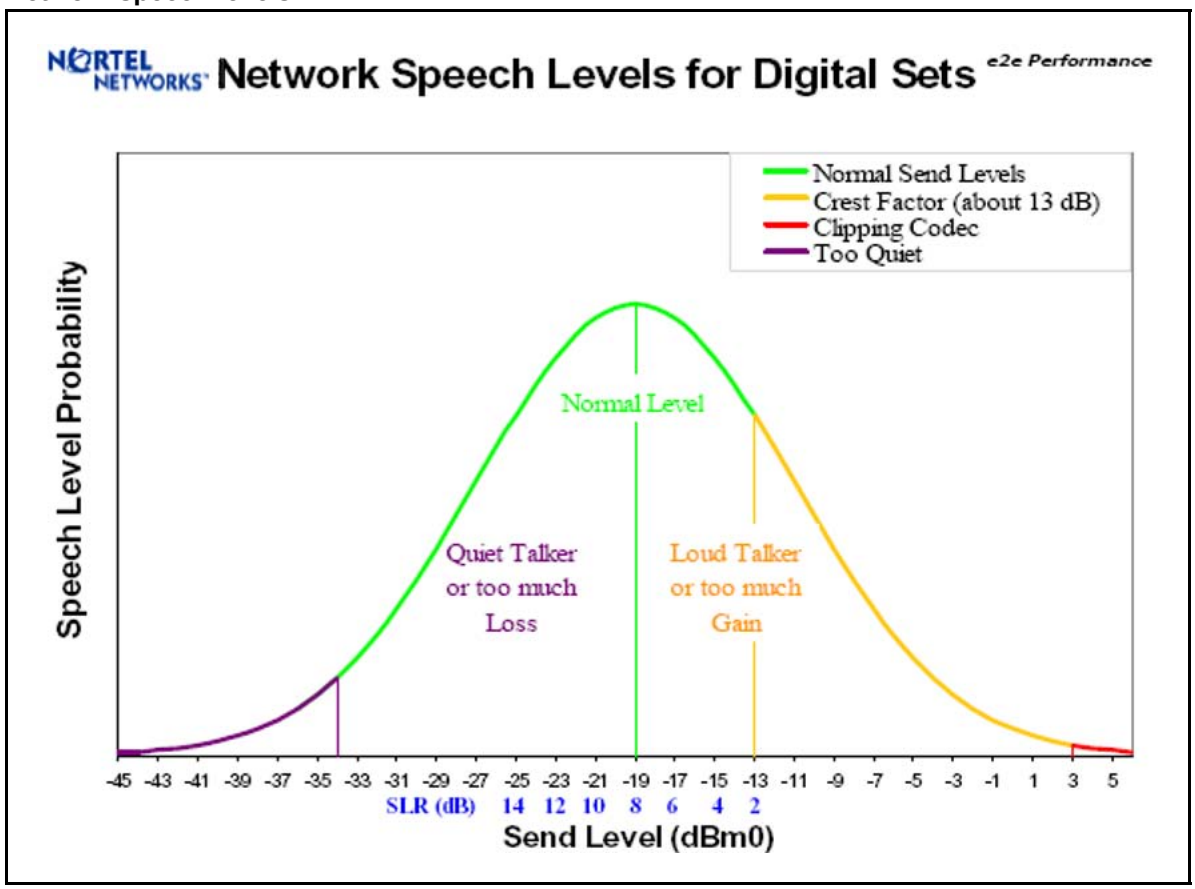
6 Call Nortel Technical Support and make arrangements to e-mail the file and error message from the display.

--End--

Network speech levels

Figure 35 "Network speech levels" (page 212) shows the network speech levels for digital sets—end-to-end performance.

Figure 35
Network speech levels


Network Speech Levels for Digital Sets
e2e Performance
Normal Send Levels
Crest Factor (about 13 dB)
Clipping Codec
Too Quiet
Speech Level Probability
Normal Level
Quiet Talker
or too much
Loss
Loud Talker
or too much
Gain
-45 -43 -41 -39 -37 -35 -33 -31 -29 -27 -25 -23 -21 -19 -17 -15 -13 -11 -9 -7 -5 -3 -1 1 3 5
SLR (dB) 14 12 10 8 6 4 2
Send Level (dBm0)

Reference documents

Table 30 "References" (page 213) lists reference documents and related-reading for this appendix.

Copyright © 2004–2008 Nortel Networks

Table 30
References

Source and type	Title	Revision	Comments
Nortel Product Bulletin	WLAN Handset 2210/2211	January 2006	Up-issue
Nortel NTP	553-3001-304	Standard 4.00 August 2005	(not applicable)
Nortel White Paper	Engineering a WLAN	(not applicable)	How to successfully deploy a WLAN
Nortel White Paper	[VoWLAN] Straight Talk on Converged Wireless LANs	(not applicable)	(not applicable)
Nortel White Paper	[QoE] Designing QoS-Enabled Networks for Voice & Data User Quality-of- Experience (QoE)	(not applicable)	(not applicable)
Nortel Technical Solution Guide	IP Telephony Client Deployment	January 2006 Version 1.0	(not applicable)
Nortel Technical Solution Guide	Solutions Guide for VoWLAN	January 2006 Version 1.0	(not applicable)
Nortel Checklist	QoS Checklist for VoWLAN using 2210 and 2211 & 2212 Handsets	Version 1.1	(not applicable)
Business Commu nications Review Article	Designing VOIP Networks: Lessons From The Edge	February 2003	(not applicable)
Nortel Configuration Guide	CS1000 & C200 Secure VOIP for SOHO & Telecommuters	1/31/2005 Version 1.1	Succession 1000 and Contivity 200 NAT traversal Solution
Nortel White Paper	Designing 802.11 Wireless LAN Networks	v1.0 December 2004	Design overview
Nortel Technical Support Bulletin	VoWLAN Implementation Best Practices	TSB- 0502001 02/01/2005	(not applicable)
SpectraLink White Paper	SpectraLink Voice Priority	5-03-edit	Quality of Service for voice traffic on wireless LANs
SpectraLink White Paper	Deploying NetLink Wireless Phones	Version 1.2.1 November 2005	Best practices

Copyright © 2004–2008 Nortel Networks

Table 30
References (cont'd.)

Source and type	Title	Revision	Comments
SpectraLink White Paper	NetLink Wireless Telephone WLAN Compatibility List	PN: 72-9000-00-W See the current version at the SpectraLink Web site.	NetLink Wireless Telephone WLAN Compatibility List
IEEE [802.11] IEEE Std 802.11	Wireless LAN Medium Access Control and Physical Layer Specifications	(not applicable)	(not applicable)
IEEE [802.11b] IEEE Std 802.11	Wireless LAN Medium Access Control and Physical Layer Specifications	(not applicable)	Higher-Speed Physical Layer Extensions in the 2.4 GHz Band
IEEE [802.11g] IEEE Std 802.11	Wireless LAN Medium Access Control and Physical Layer Specifications	(not applicable)	Further Higher Data Rate Extension in the 2.4 GHz Band
SpectraLink White Paper	Cisco 1100-1200- 1300 AP config/deploy guide	PN: 72-9962-00-A	(not applicable)
SpectraLink Configuration Note	Cisco Aironet 350/1100/1200 (DS) AP – IOS Operating System	PN: 72-9975-00-C beta	(not applicable)
SpectraLink Configuration Note	CISCO AP Setup for external radius for FSR	(not applicable)	(not applicable)
SpectraLink Configuration Note	CISCO external radius setup for FSR	(not applicable)	(not applicable)
SpectraLink Configuration Note	Airespace Wireless Enterprise Platform – AireOS	72_9974_00_B.pdf	Updated AUTORF settings

Copyright © 2004–2008 Nortel Networks

Appendix
Compatible Access Points

The Nortel Voice over Wireless LAN solution is supported on VIEW-certified Access Points (APs).

For a list of certified APs, go to the SpectraLink Web site www.spectralink.com. On the home page, select RESOURCES > Wi-Fi COMPATIBILITY.

The SpectraLink Web site also contains configuration notes for the compatible APs.

Copyright © 2004–2008 Nortel Networks

Copyright © 2004–2008 Nortel Networks

Index

10 Mbs 66
50 ms 74
70 ms 74
802.1 pq 77
802.1p tagging 77

A

Access Points (APs)
Compatible 215
Administration Console navigation 148
alarms 114
alarms on the WLAN IP Telephony Manager 2245 114
alarms, active 114
AP
configuration 186

C

Call Server 105
CFNA 118
checking in 105
Cisco 171
4400 Series WLAN Controller 172
Aironet 1200 series 171
Aironet 1200 Series 187
configuration examples 174
Codecs 73–74
Components 20
CS 1000 84

D

DHCP 67
options 178
server options 177
DiffServ 77
duplex mismatch 39, 116, 118

E

echo 118
Error Status screen 114
External Applications Server 77

F

filters 59
Full-duplex 39

G

G.711 73
G.723.1 74
G.729A 73
G.729B 73
Gain adjustment 75
gateway 57, 77, 105–106

H

half-duplex 66

I

ISM parameters 20

J

jitter 74
jitter buffer 73–74

L

Language 20
latency 74
Layer 2 port 77
Layer 2 QoS 77
Layer 2 switch port 77
Layer 3 port 77

Copyright © 2004–2008 Nortel Networks

locking the WLAN IP Telephony Manager 2245 108
loss plan 75
LTPS 105

M

multicast addresses 58
Multicasting 58

N

network segments 59
No ring 118
node 74
Nortel
  WLAN Security Switch 171
Nortel WLAN Security Switch 2270 172

P

packet loss 74
Planning worksheets 68
prevent new calls from starting 108
priority 77
Programmable rings and tones 75
Push-to-talk (PTT) 21, 58

Q

Quality of Service
  checklist 184

R

rack-mount unit 67
Receive Loudness Rating (RLR) 74
refresh 31
remote endpoint 74
reset the WLAN IP Telephony Manager 2245 108
RF
  basics 186
RLR 74
Roaming 57
Routers 59
RTCP 74
RTP 73

S

Security
  Virtual Private Network (VPN) 21
  Wi-Fi Protected Access (WPA) 21
  Wi-Fi Protected Access2 (WPA2) 21
  Wired Equivalent Privacy (WEP) 21
Send Loudness Rating (SLR) 74
site data-gathering
  tables 167
SLR 74
software updates 107
software versions 107
subnet 59
SVPServer
  Mounting 90
switches
  configuration 171

T

TFTP 107
Timing function 57
tone capability 75
troubleshooting 39, 105

U

UNIStim 73, 77
unzipped 31
Update software 107

V

Virtual Private Network (VPN) 21
VLAN 59
voice mail 118

W

Wi-Fi Protected Access (WPA) 21
Wi-Fi Protected Access2 (WPA2) 21
Wired Equivalent Privacy (WEP) 21
WLAN
  configuration 176
WLAN applications 184

Copyright © 2004–2008 Nortel Networks

Nortel Communication Server 1000

WLAN IP Telephony Installation and Commissioning

Copyright © 2004–2008 Nortel Networks
All Rights Reserved.

Release: 5.5
Publication: NN43001-504
Document status: Standard
Document revision: 03.04
Document release date: 23 September 2008

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com
Sourced in Canada

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.